Exhibit A

Proposed Reliability Standard

CIP-003-7 Clean Version

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-7

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. 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 SPS or RAS where the SPS or 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-003-7:

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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3. 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.

4.2.3.4. 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-003-7.

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation; 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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1)	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1)	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the six topics required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 within 15 calendar	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the six topics required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 within 16 calendar	BES Cyber Systems, but did not address three of the six topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) 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 BES Cyber Systems 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	months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) 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 BES Cyber Systems 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	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.2)	calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2,	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing	to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but	access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR The Responsible Entity documented the determination of	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented	failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber	the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Assets and Removable Media, but 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 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2,		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 5.3. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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.	

Version	Date	Action	Change Tracking
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 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.

Attachment 1

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

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

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

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

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

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

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

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the

Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

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

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

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

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, the use of one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

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

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

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

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

Attachment 2

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

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

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

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

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

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

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

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

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

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability

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.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents

- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media
- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a

combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such

communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located

at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

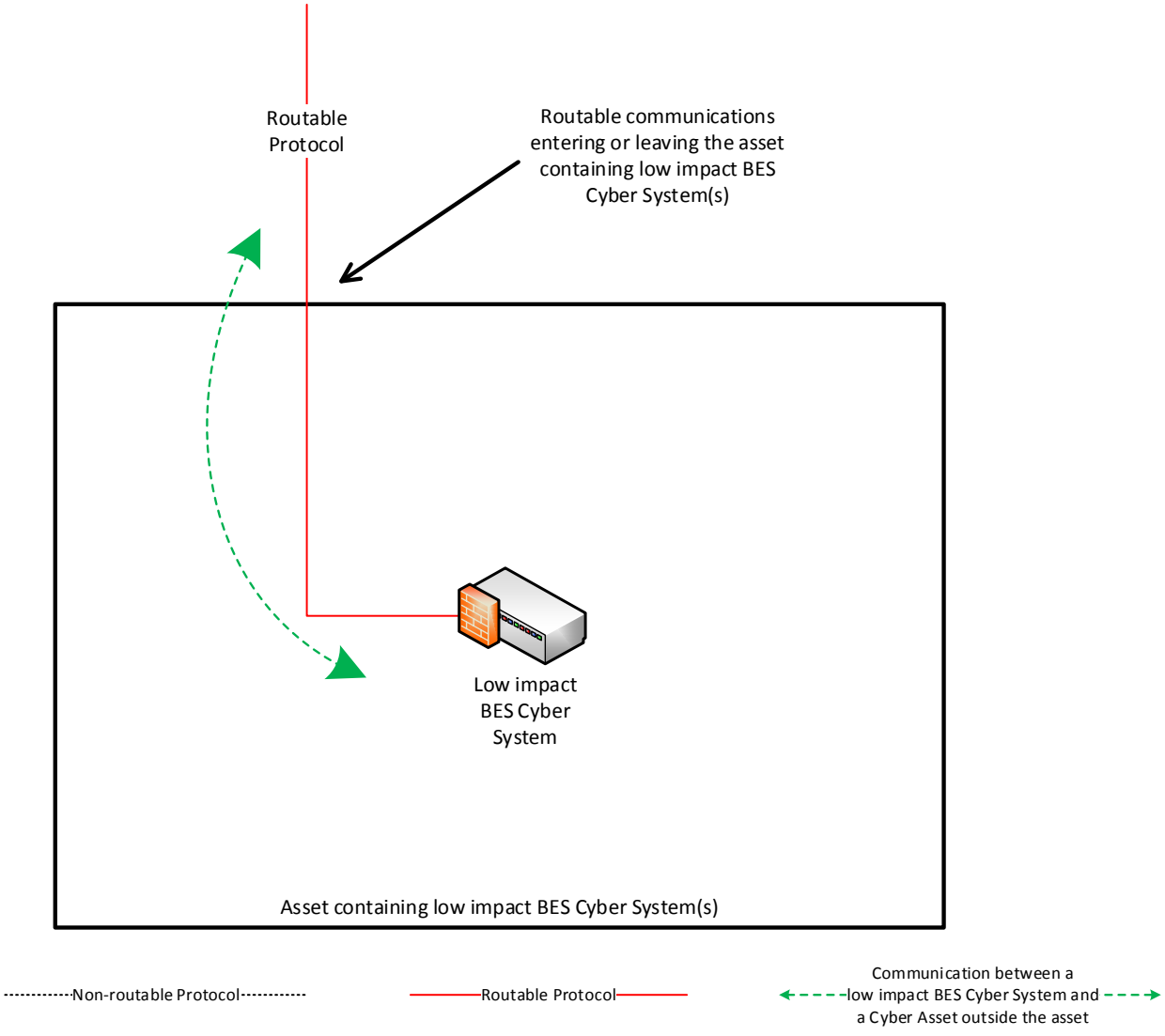
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

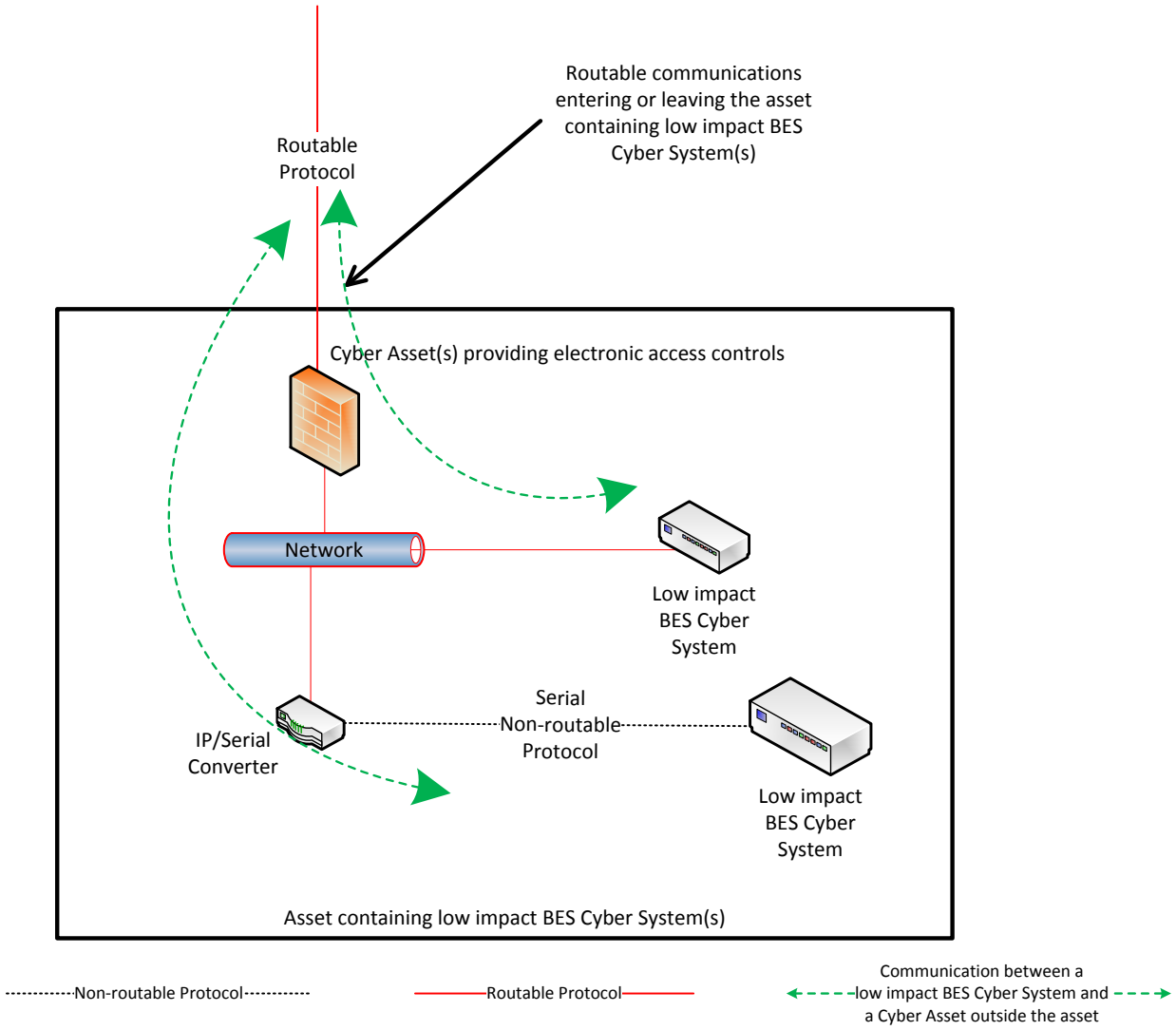
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

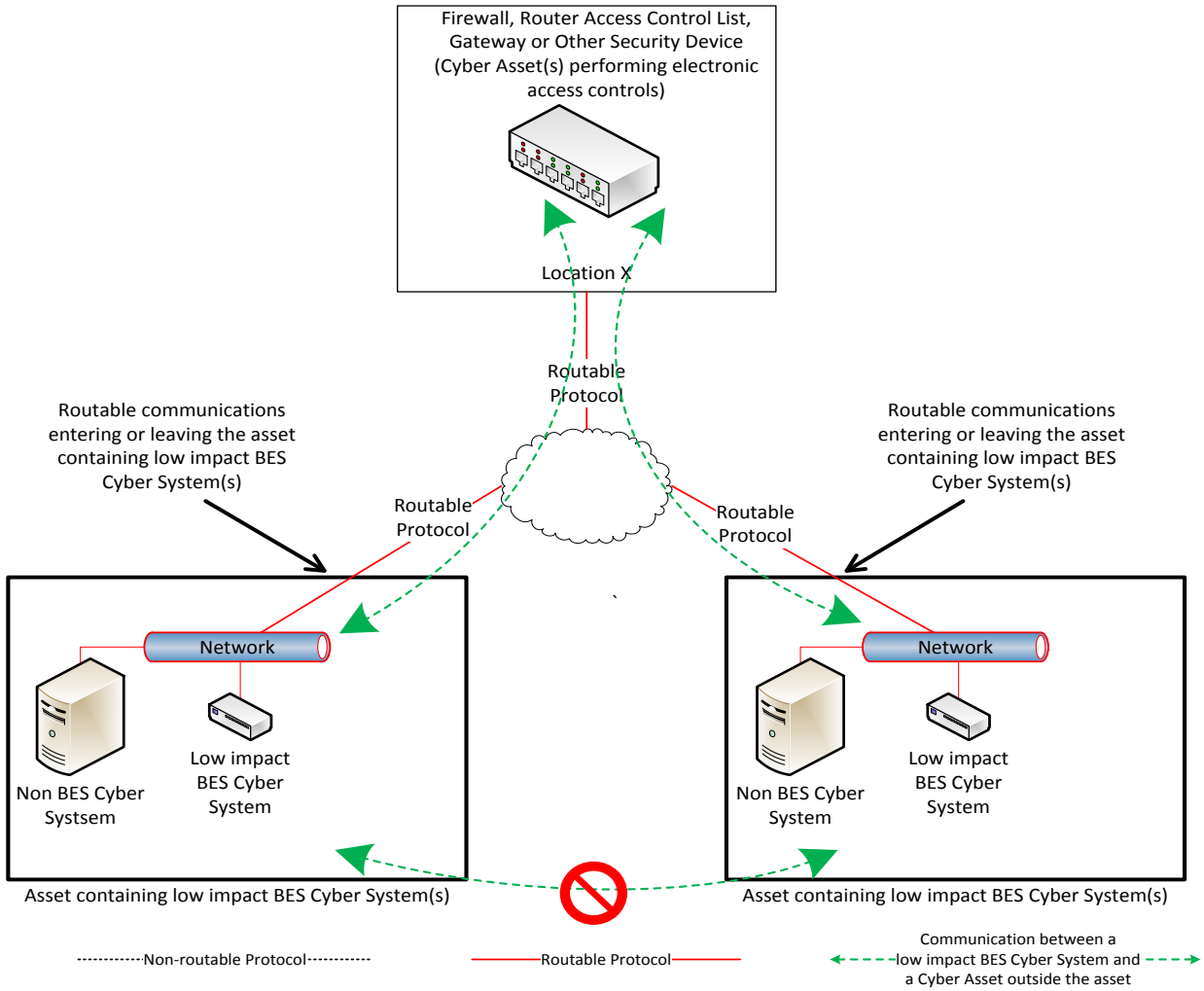
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

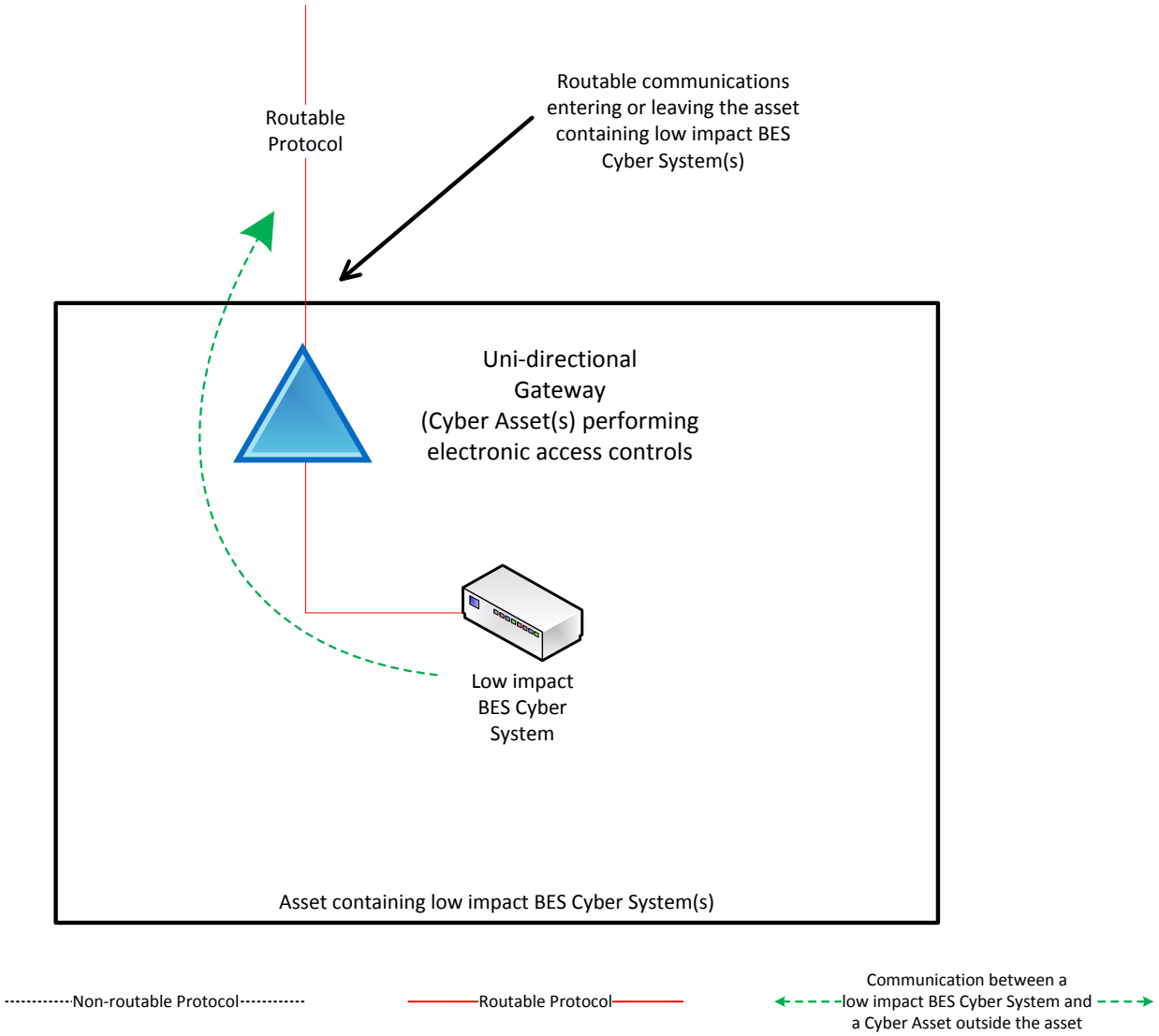
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

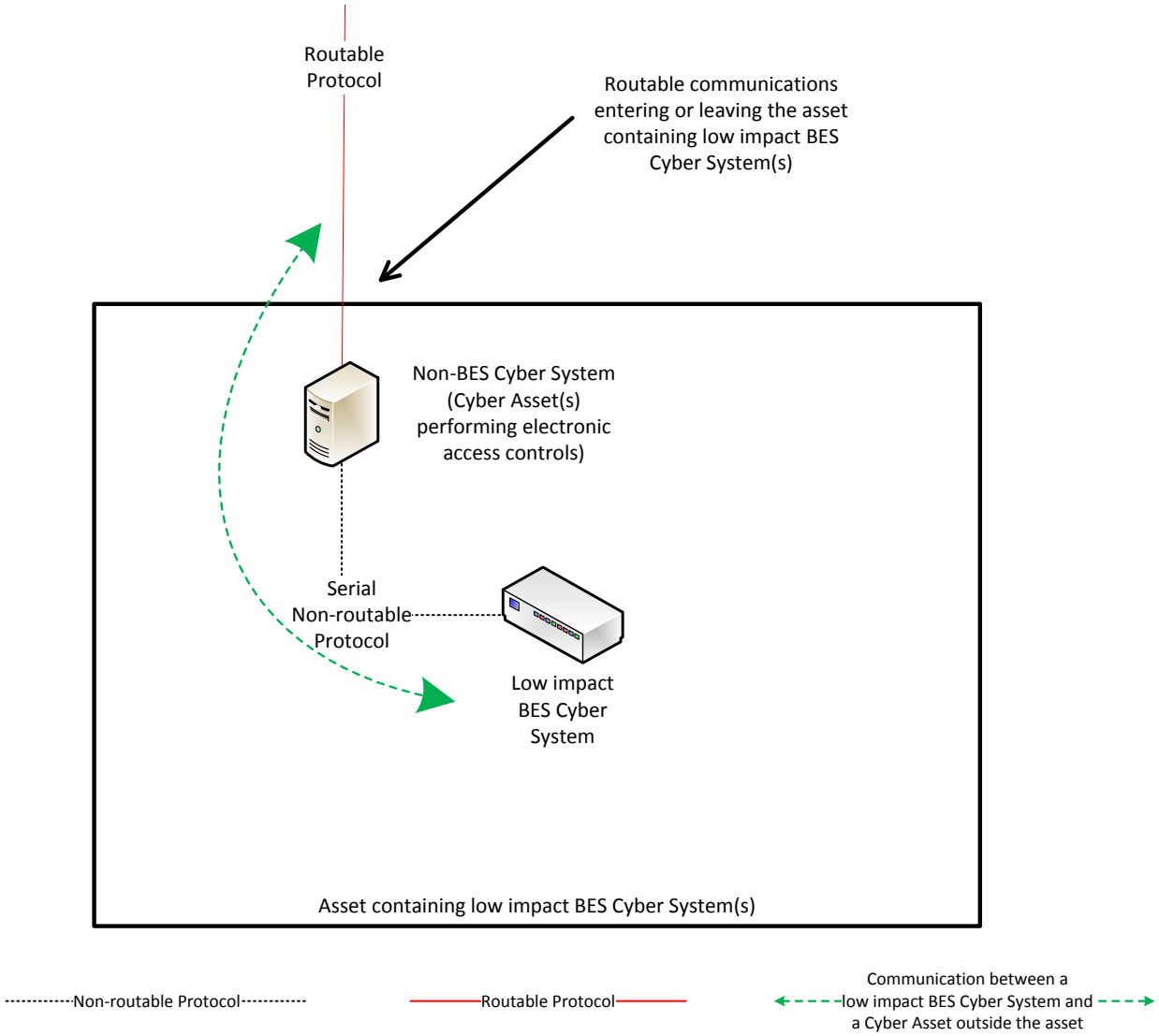
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

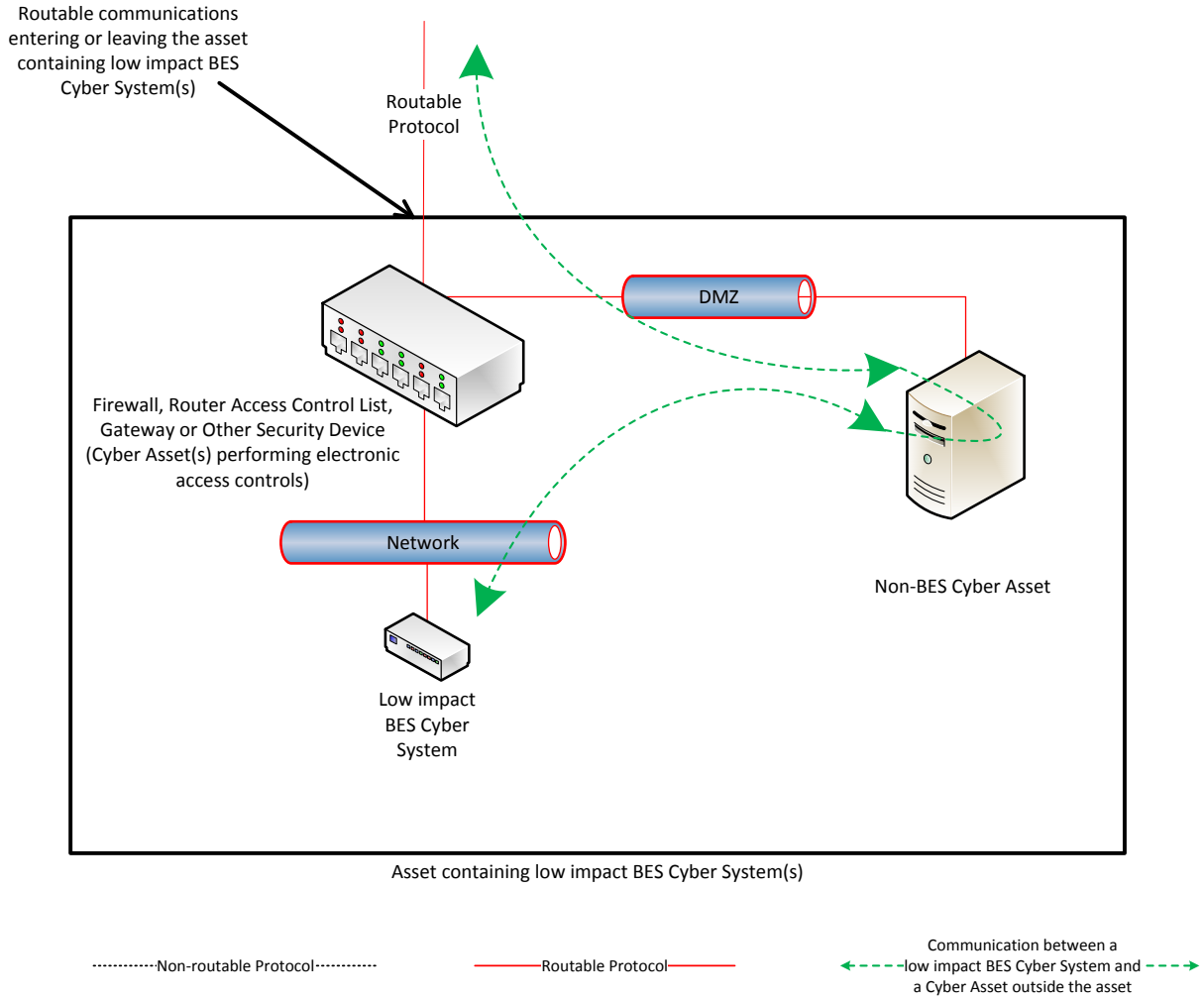
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

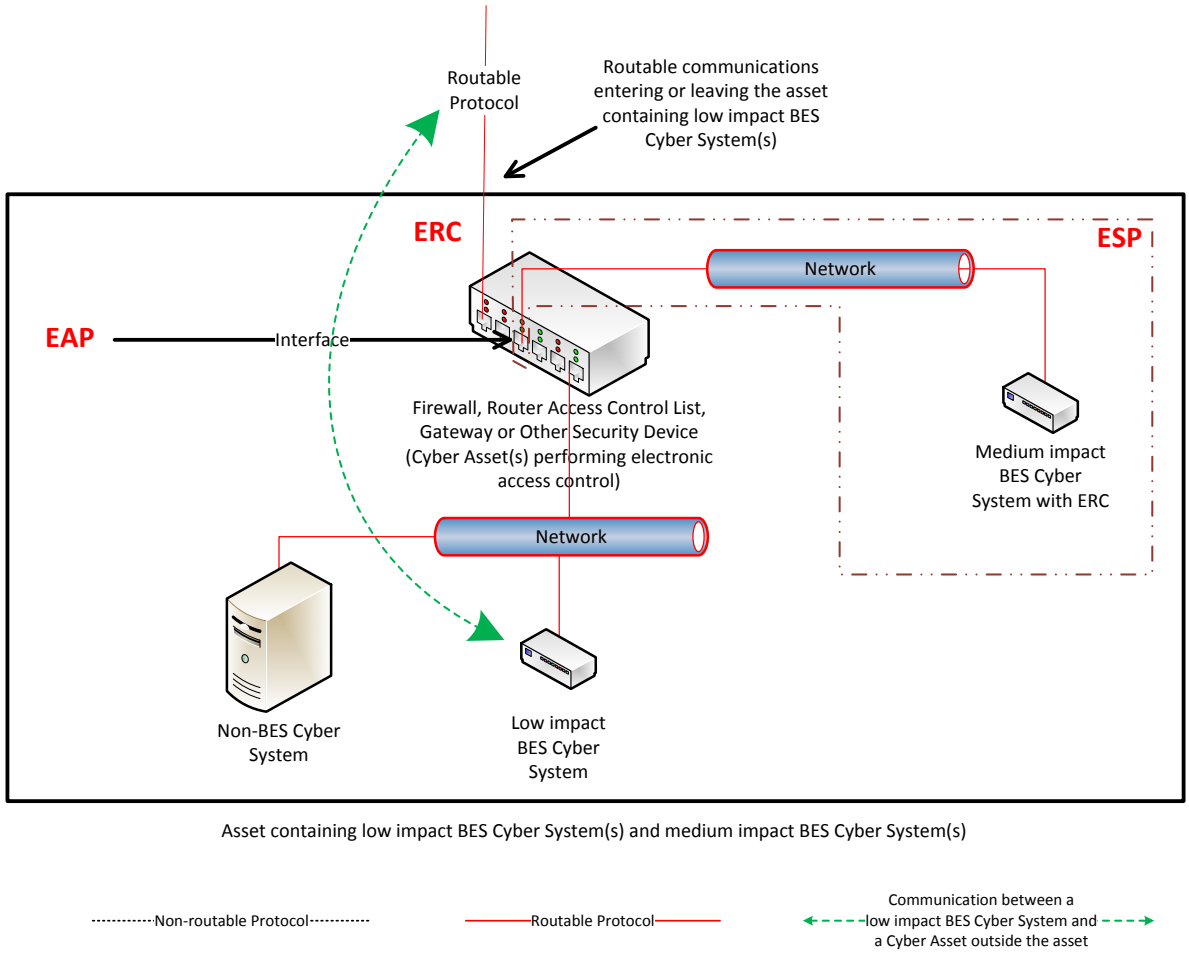
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.

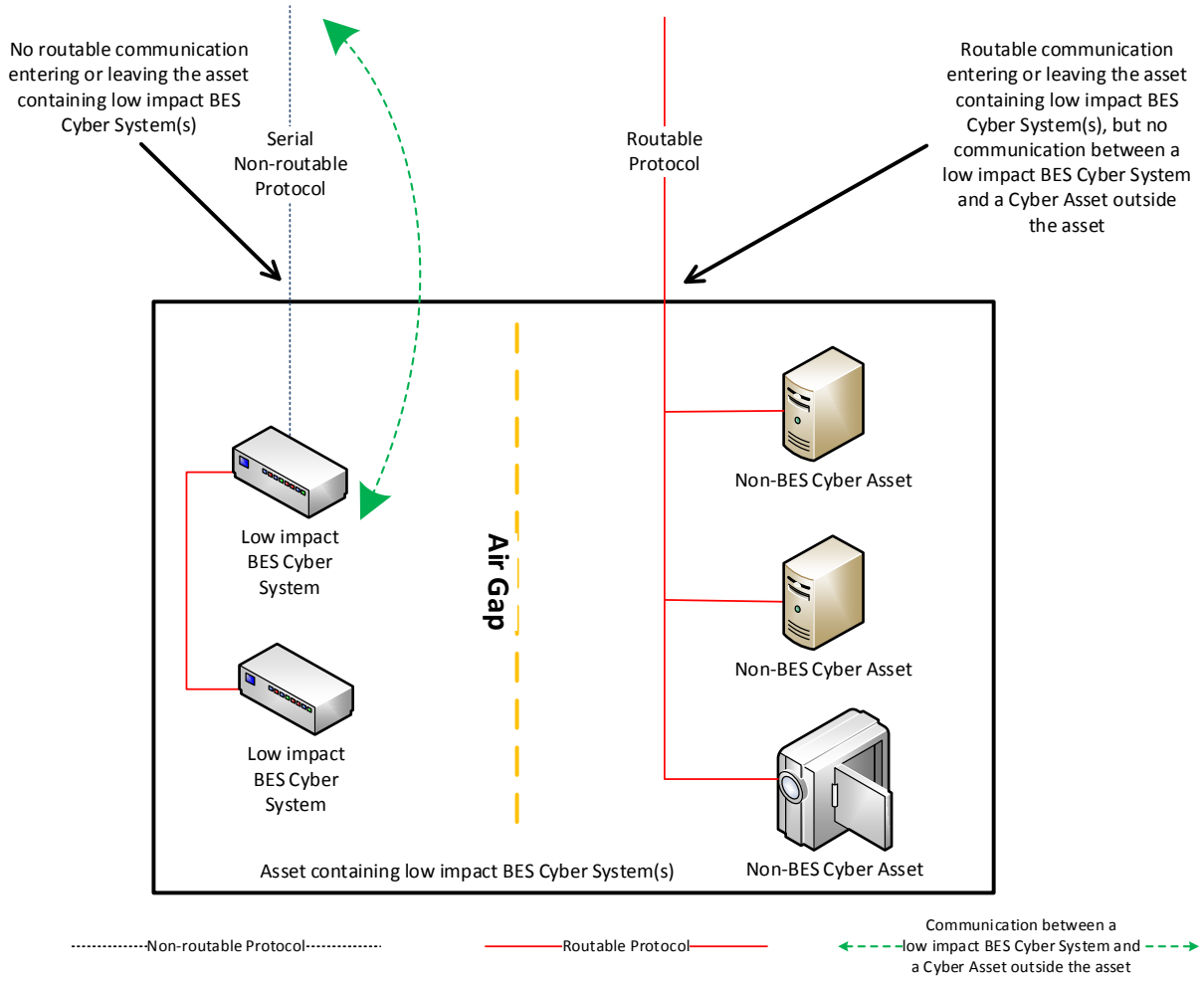


Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

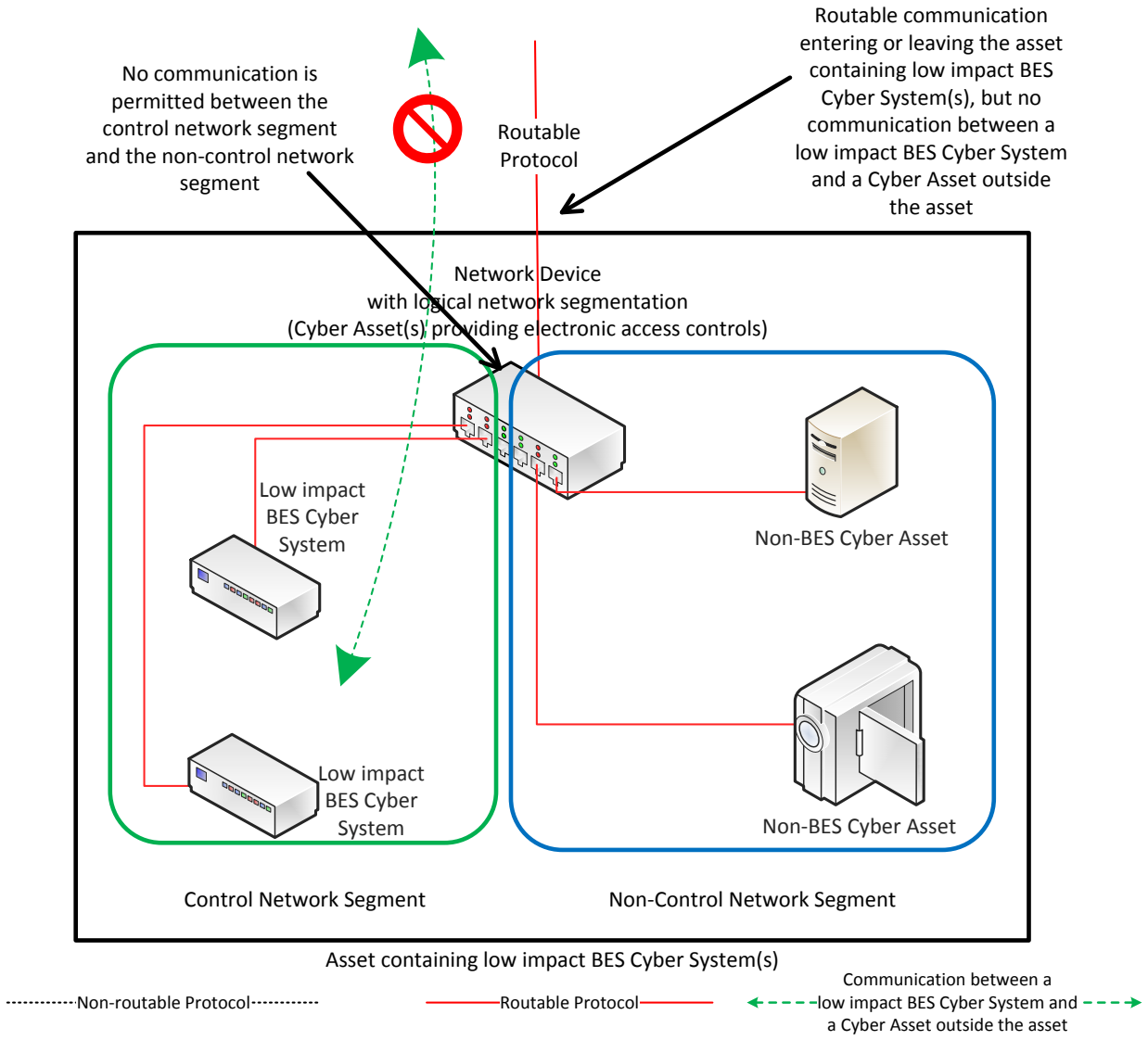
1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

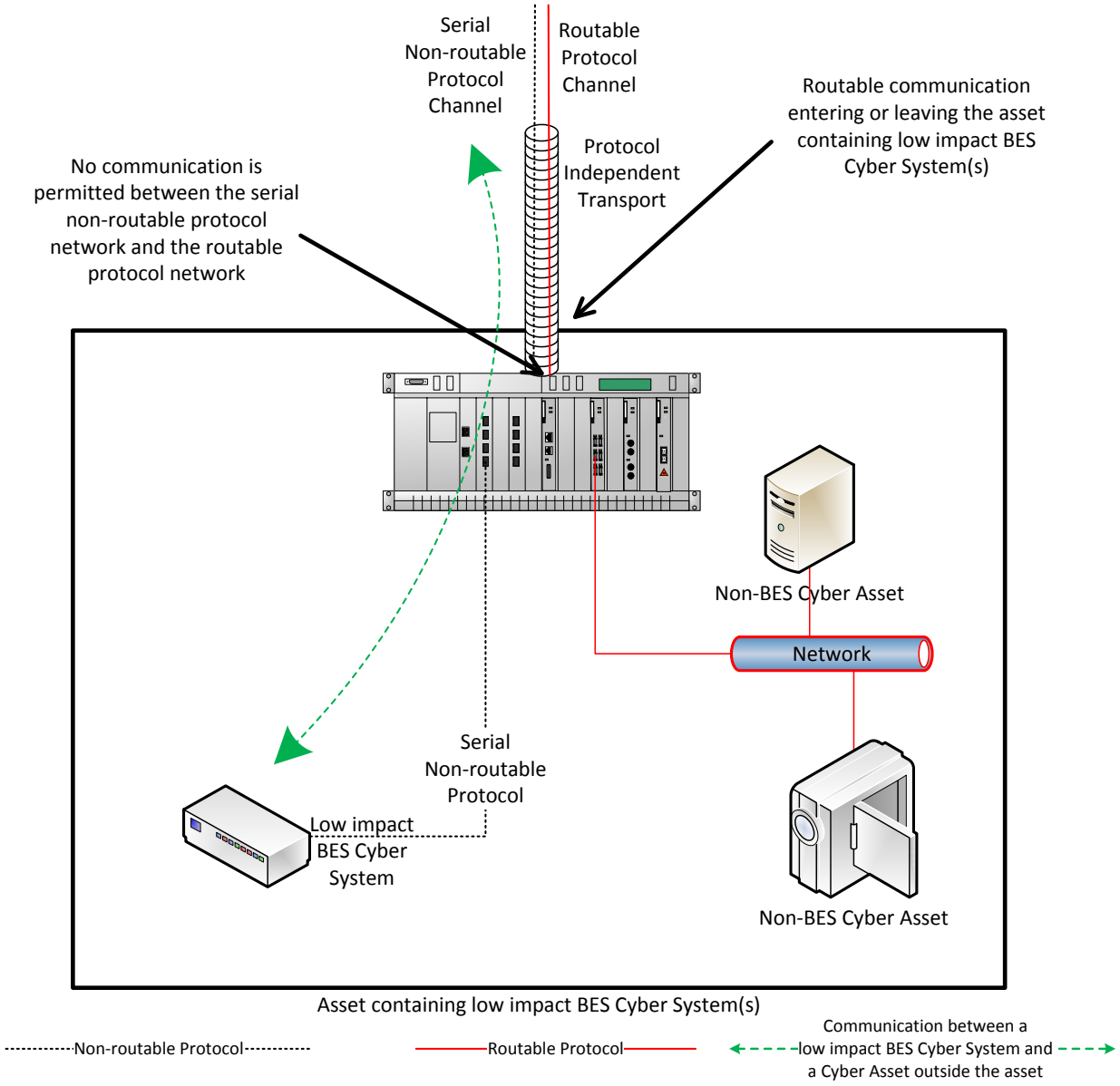
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Malicious Code Risk Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that

can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition

and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

Rationale for Section 5 of Attachment 1 (Requirement R2):
Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

CIP-003-7 Redline Version

A. Introduction

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

2. **Number:** CIP-003-~~6~~7

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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. Interchange Coordinator or Interchange Authority

   4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. 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 SPS or RAS where the SPS or 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-~~6:~~ 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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3. 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.

4.2.3.4. 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-~~6~~7.

6. ~~6.~~ Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls ~~for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and~~;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets 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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the ~~four~~six topics required by R1. (R1.2) 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 BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the ~~four~~six topics required by R1. (R1.2) 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 BES Cyber Systems as	BES Cyber Systems, but did not address three of the ~~four~~six topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address ~~any~~four or more of the ~~four~~six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	Systems as required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but	The Responsible Entity failed to document ~~or~~and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to ~~CIP-003-6,~~ Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response ~~plans~~plan(s) according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident	containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented	failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response ~~plans~~plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			response ~~plans~~plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2,	its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response ~~plans~~plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for	OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~E-ISAC) according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented ~~and implemented electronic access controls~~its plan(s) for ~~LERC~~Transient Cyber Assets and Removable Media, but failed to implement ~~a LEAP or permit inbound and~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	identification, classification, and response to Cyber Security Incidents according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR ~~(R2)~~ ~~OR~~ The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent	~~outbound access~~ mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section ~~3~~5.1. (R2) OR The Responsible Entity documented ~~and implemented electronic access controls~~its plan(s) for ~~its assets containing low impact BES~~Transient Cyber ~~Systems~~Assets and Removable Media, but failed to ~~document and~~ implement ~~authentication of all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems~~mitigation for the introduction of	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				notification to the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ESE~~-ISAC) according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its ~~cyber security~~ plan(s) for ~~its assets containing low impact BES~~Transient Cyber ~~Systems~~Assets and Removable Media, but failed to document ~~physical security controls~~ mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible	malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section ~~3~~5.2. (R2) OR The Responsible Entity documented ~~the physical access controls~~its plan(s) for ~~its assets containing low impact BES~~Transient Cyber ~~Systems~~Assets and Removable Media, but failed to implement ~~the physical security controls~~mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to ~~CIP-~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Entity according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, ~~Section 2.~~ Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its ~~cyber security~~ plan(s) for ~~its assets containing low impact BES~~Transient Cyber ~~Systems~~Assets and Removable Media, but failed to document ~~electronic access controls~~mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to ~~CIP-003-6,~~Requirement	~~003-6,~~ Requirement R2, Attachment 1, Section ~~2~~5.3. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			40 calendar days of the change. (R3)	change in less than 50 calendar days of the change. (R3)		Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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.	

Version	Date	Action	Change Tracking
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 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.

Attachment 1

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

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

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

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

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

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

Section 3. ~~For LERC, if any,~~ implement ~~a LEAP to permit~~electronic access controls to:

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

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

~~i.~~ii. using a routable protocol ~~access;~~when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. ~~Implement authentication for~~not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~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.

~~CIP-003-6 - Attachment 2~~

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

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

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

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, the use of one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

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

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

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

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

Attachment 2

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

Section 1. ~~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. ~~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 BES Cyber Systems within the asset; and

~~b.~~ The Cyber Asset~~, if any, containing a LEAP.~~

b. (s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3~~.~~.1, if any.

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

1. ~~Documentation showing that inbound and outbound connections for any LEAP(s) are confined to only those the Responsible Entity deems necessary (e.g., by restricting IP addresses, ports, or services); and documentation~~Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of

inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

~~1.~~2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2 may include, but are not limited to, documentation from change management systems, electronic mail or

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

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.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-~~6~~7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-~~6~~7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the ~~four~~six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-~~6~~7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity ~~should~~may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents

- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media
- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

~~Using the list of assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement~~The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that ~~addresses~~address the security objective ~~criteria~~ for the protection of low impact BES Cyber Systems. ~~The protections required by Requirement R2 reflect the level of risk that misuse or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the~~The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively ~~either~~ at an asset ~~or site~~ level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

~~There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and **Dial-up Connectivity**, and (4) Cyber Security Incident response.~~

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the ~~four~~ subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible ~~Entity is not~~Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems ~~at assets containing low impact BES Cyber System(s)~~ within the asset, and (2) ~~LEAPs~~Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If ~~the LEAP is~~these Cyber Assets implementing the electronic access controls are located within the ~~BES asset and inherits the~~ same ~~controls~~ asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this ~~can~~may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility in the selection ofto select the methods used to meet the objective to control of controlling physical access to (1) the asset(s) containing low impact BES Cyber Systems,System(s) or the low impact BES Cyber Systems themselves, or LEAPs and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level for access to the site or systems, including LEAPs.. The requirement doesstandard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of a usera individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). TheThe standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of boundary protectionselectronic access controls for assets containing low impact BES Cyber Systems when the low impact BES Cyber Systems have bi-directionalthere is routable protocol communication or Dial-up Connectivity to devices external to between Cyber Asset(s) outside of the asset containing the low impact BES Cyber Systems. The establishment of boundary protections is intended to control communication either into the asset containing low impact BES Cyber System(s) or toand the low impact BES Cyber System itself to (s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. The term "electronic access control" is used in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing. The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or Dial-up Connectivity present. In the case where there is no external bi-directional routable protocol communication or Dial-up Connectivity, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s).

~~The defined terms LERC~~When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and ~~LEAP~~outbound electronic access are ~~used to avoid confusion with the similar terms used~~required for ~~high~~communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and ~~medium~~when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems ~~(e.g., External Routable~~that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity ~~(ERC) or~~ to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access ~~Point (EAP)). To future-proof the standards, and in~~Control Exclusion

In order to avoid future technology issues, the ~~definitions specifically~~obligations for electronic access controls exclude ~~"point-to-point~~ communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions ~~between Transmission station or substation assets containing low impact BES Cyber Systems,",~~ such as IEC TR-61850-90-5 R-GOOSE messaging. ~~This does not exclude Control Center communication but rather excludes the communication between the intelligent electronic devices themselves.~~Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement ~~a~~

LEAP.the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive requirementscharacteristics related to this technology norand not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

When determining whether **Considerations for Determining Routable Protocol Communications**

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is LERC to the low impact BES Cyber System, the definition uses the phrases "direct user-initiated interactive access or a direct device-to-device connection to communication between a low impact BES Cyber System(s) fromand a Cyber Asset(s) outside the asset containing thosethe low impact BES Cyber System(s) viathat uses a routable protocol when entering or leaving the asset.

When determining whether a bi-directional routable protocol connection." The intent of "direct" in the definition is to indicate LERC exists if a person is sitting at another device outside ofentering or leaving the asset containing the low impact BES Cyber System, and (s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session even if there is a serial-to-routable protocol conversion. The reverse case would also be LERC, in which the individual sits at thecommunication entering or leaving the asset between a low impact BES Cyber System and connects Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to a device be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing

the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

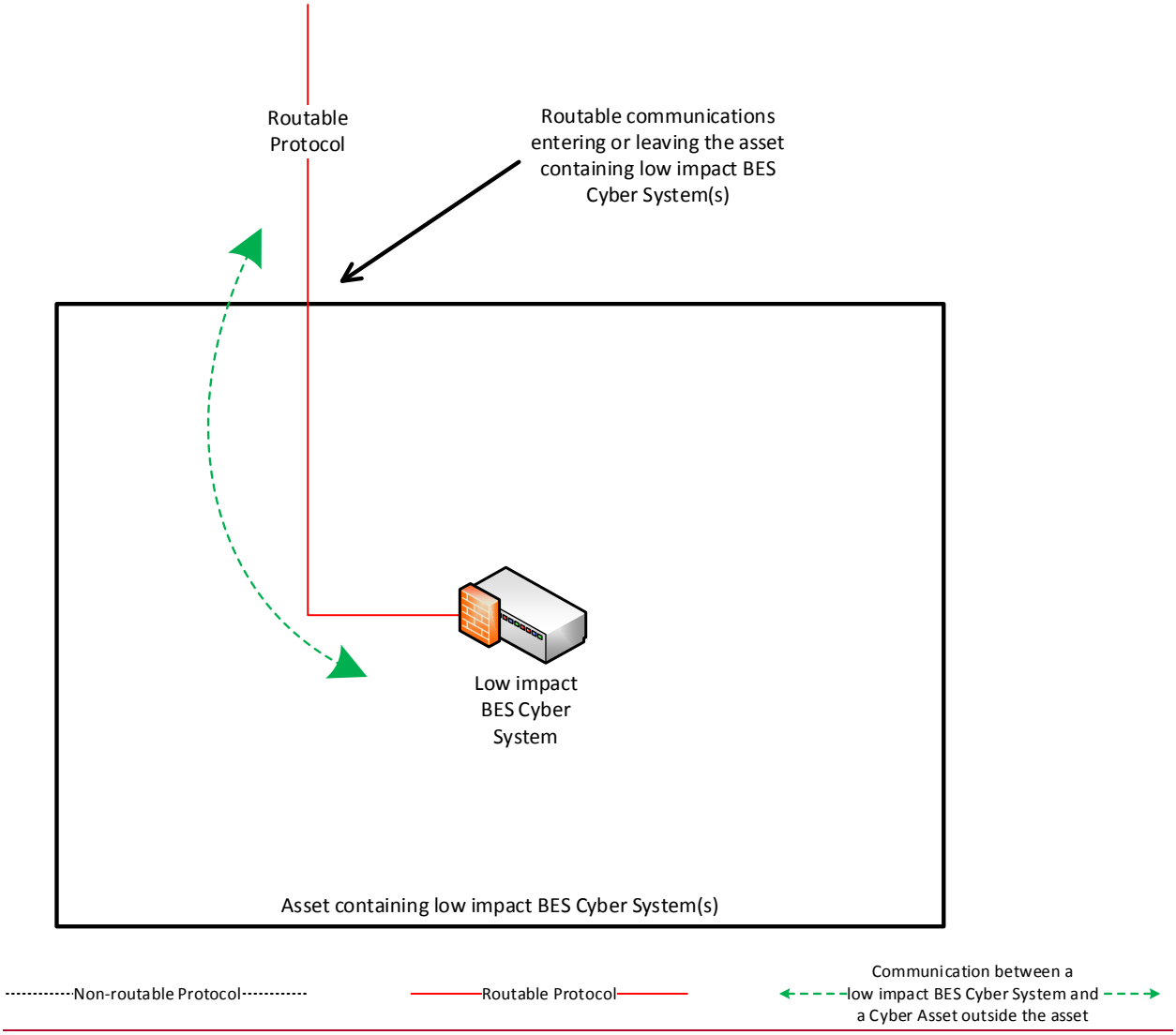
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

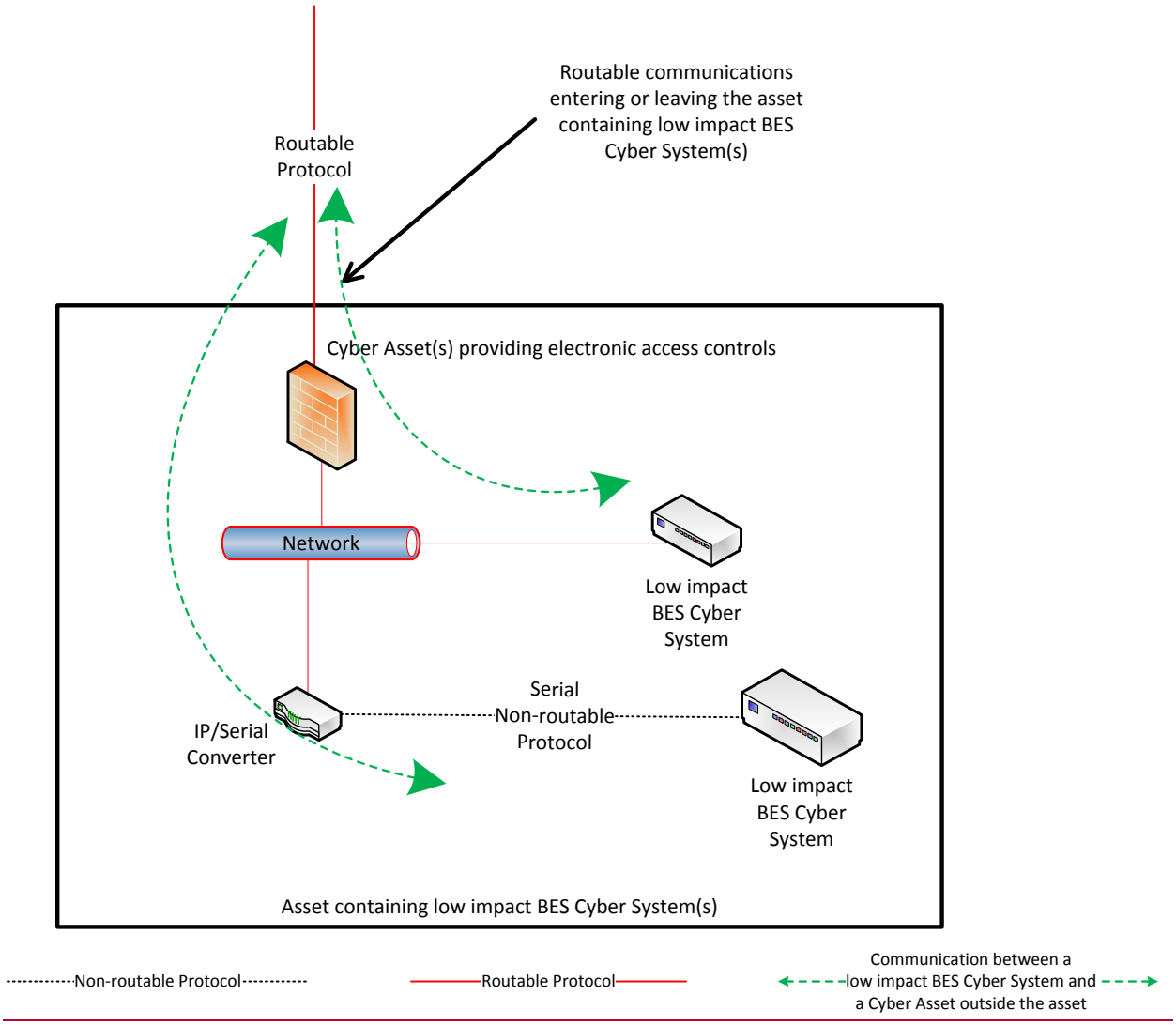
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

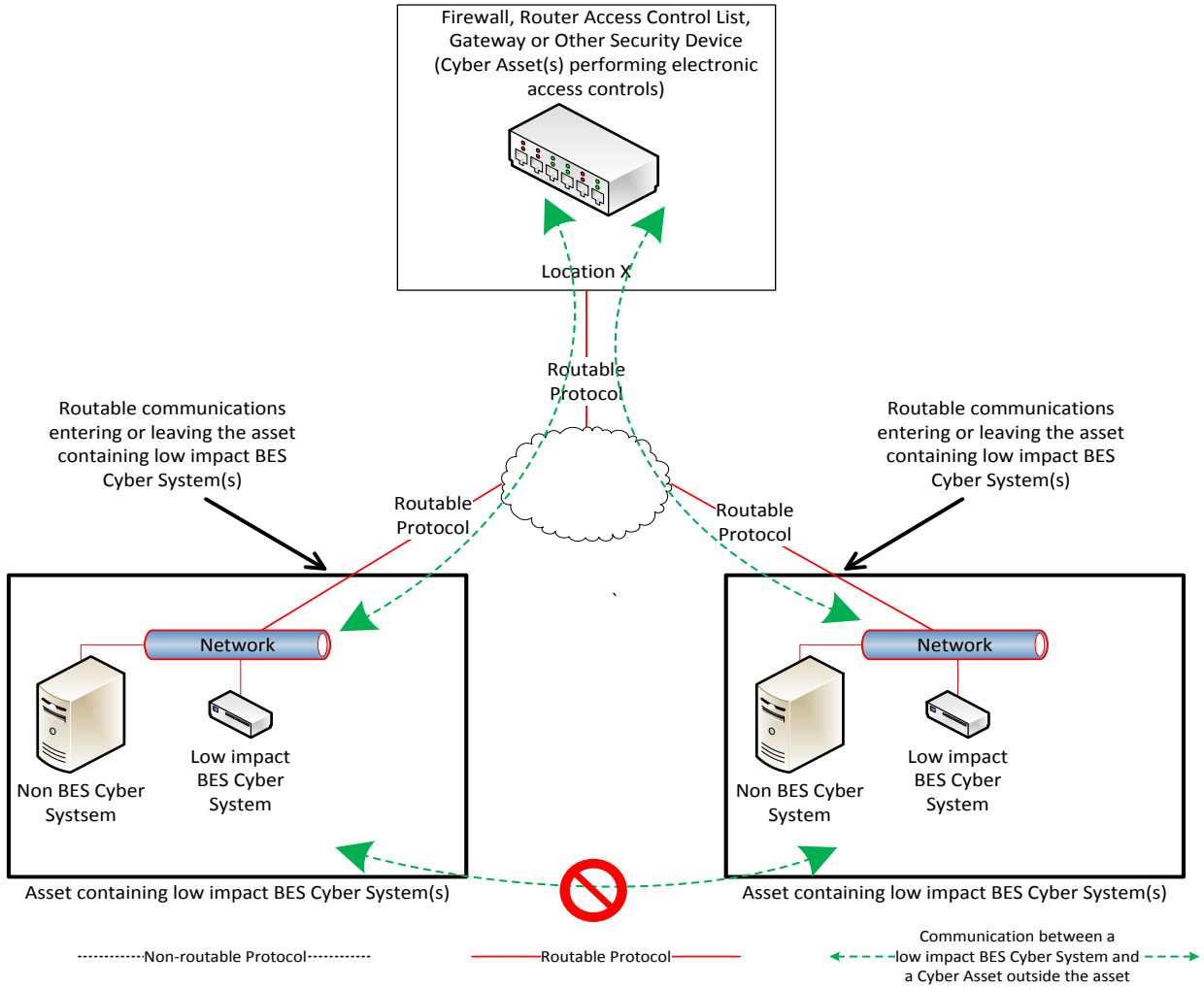
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

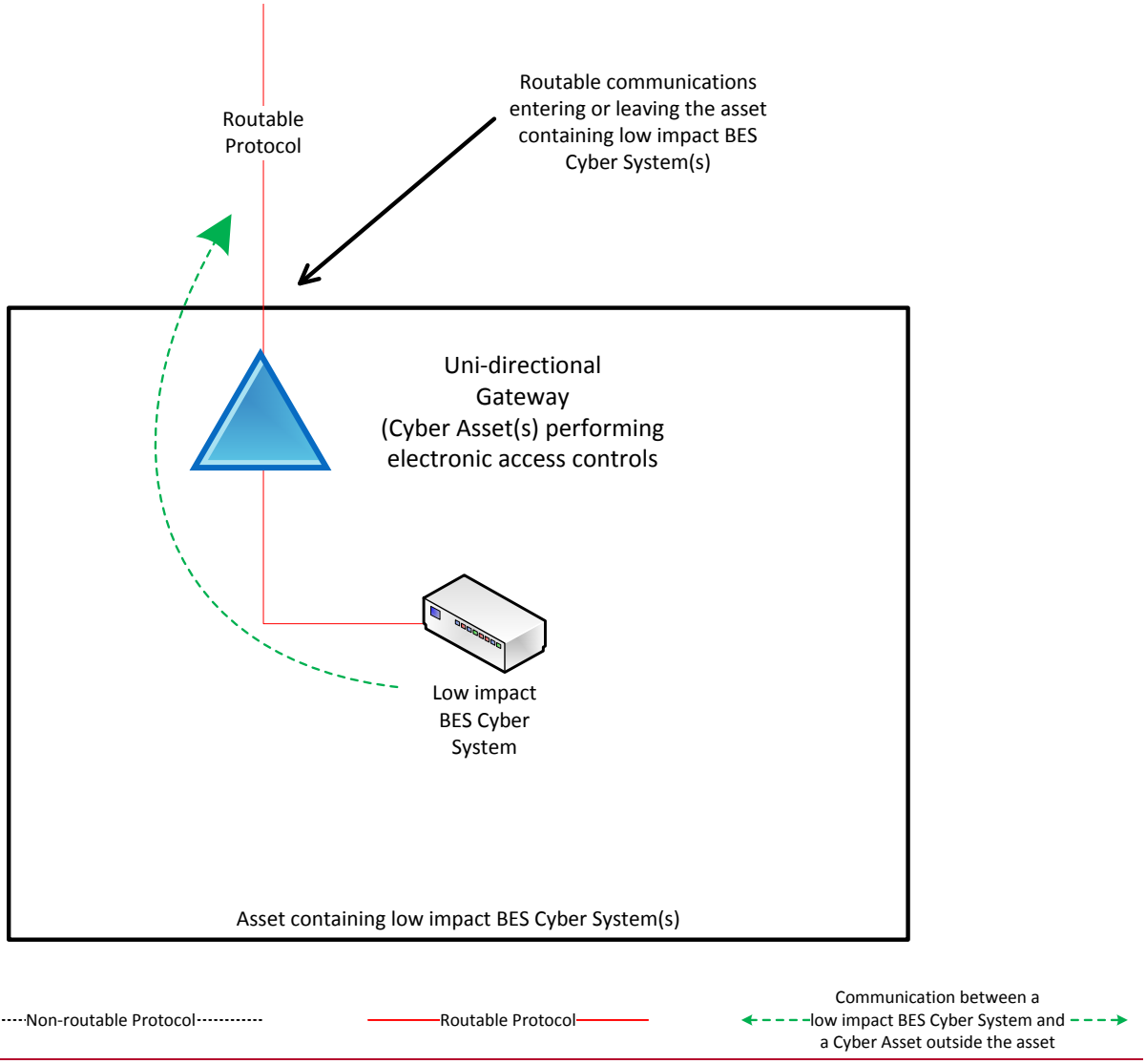
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

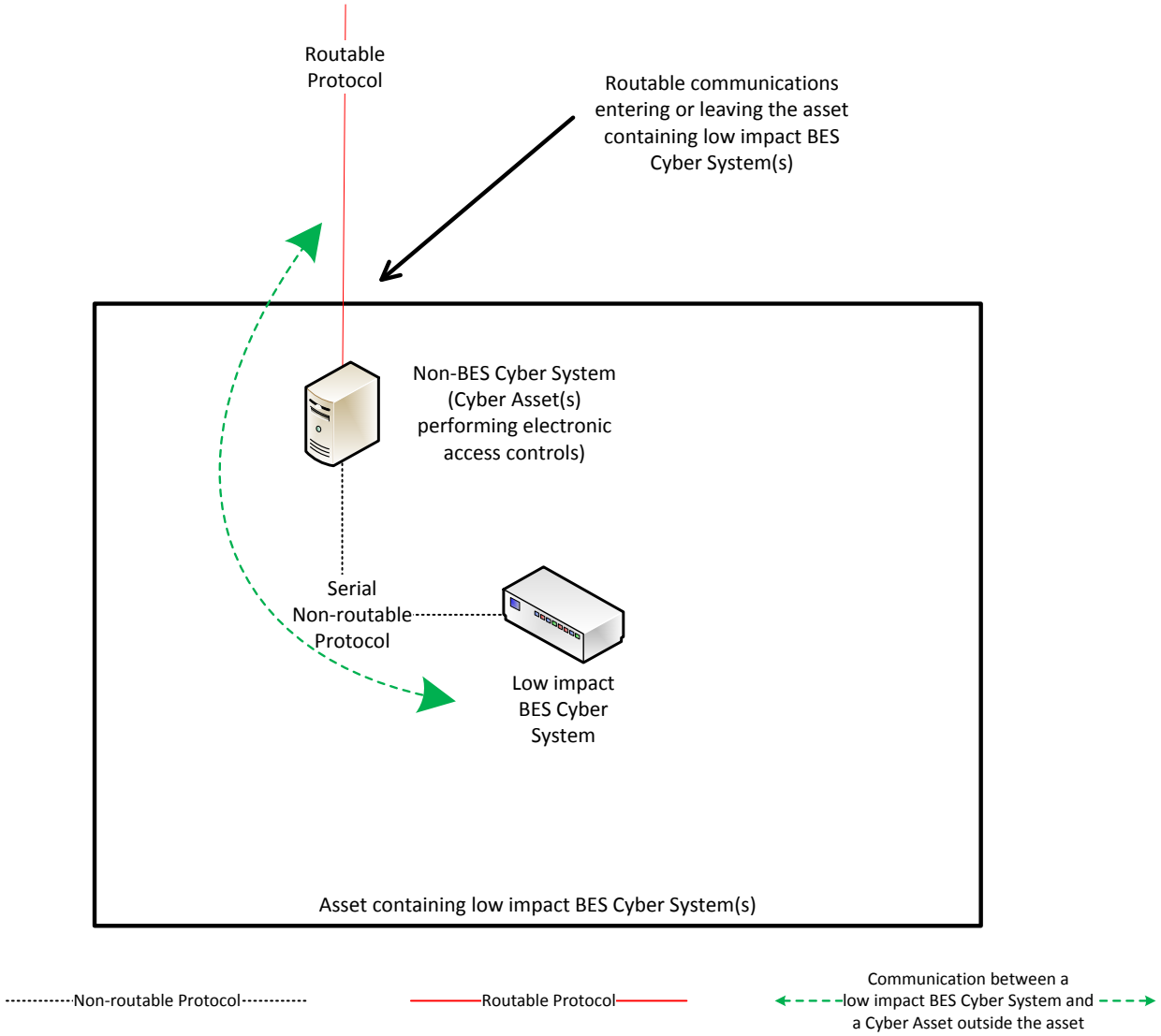
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4 ~~*Systems using a single end-to-end bi-directional routable protocol session. Additionally, for "device-to-*~~

Reference Model 5 – User Authentication

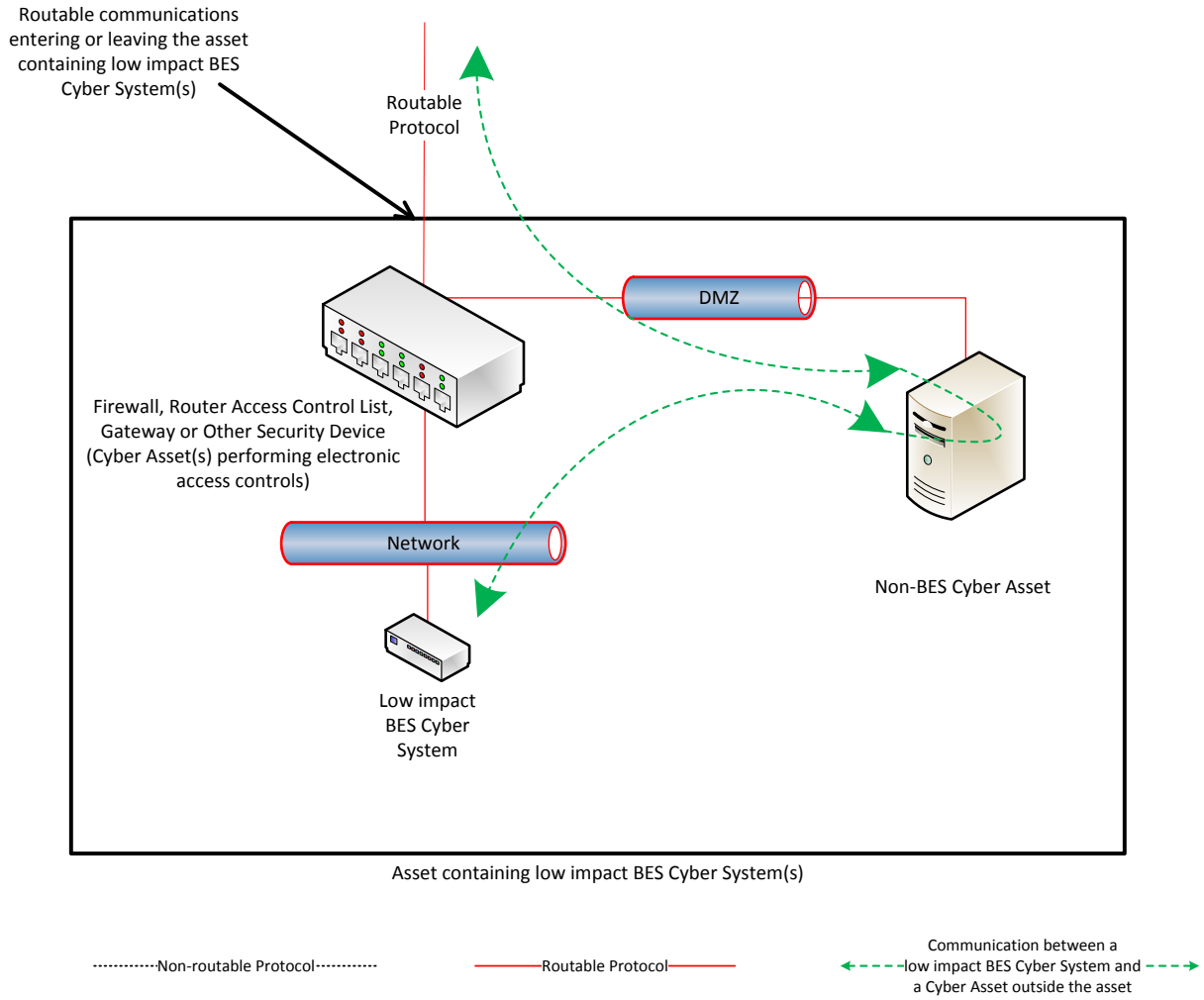
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

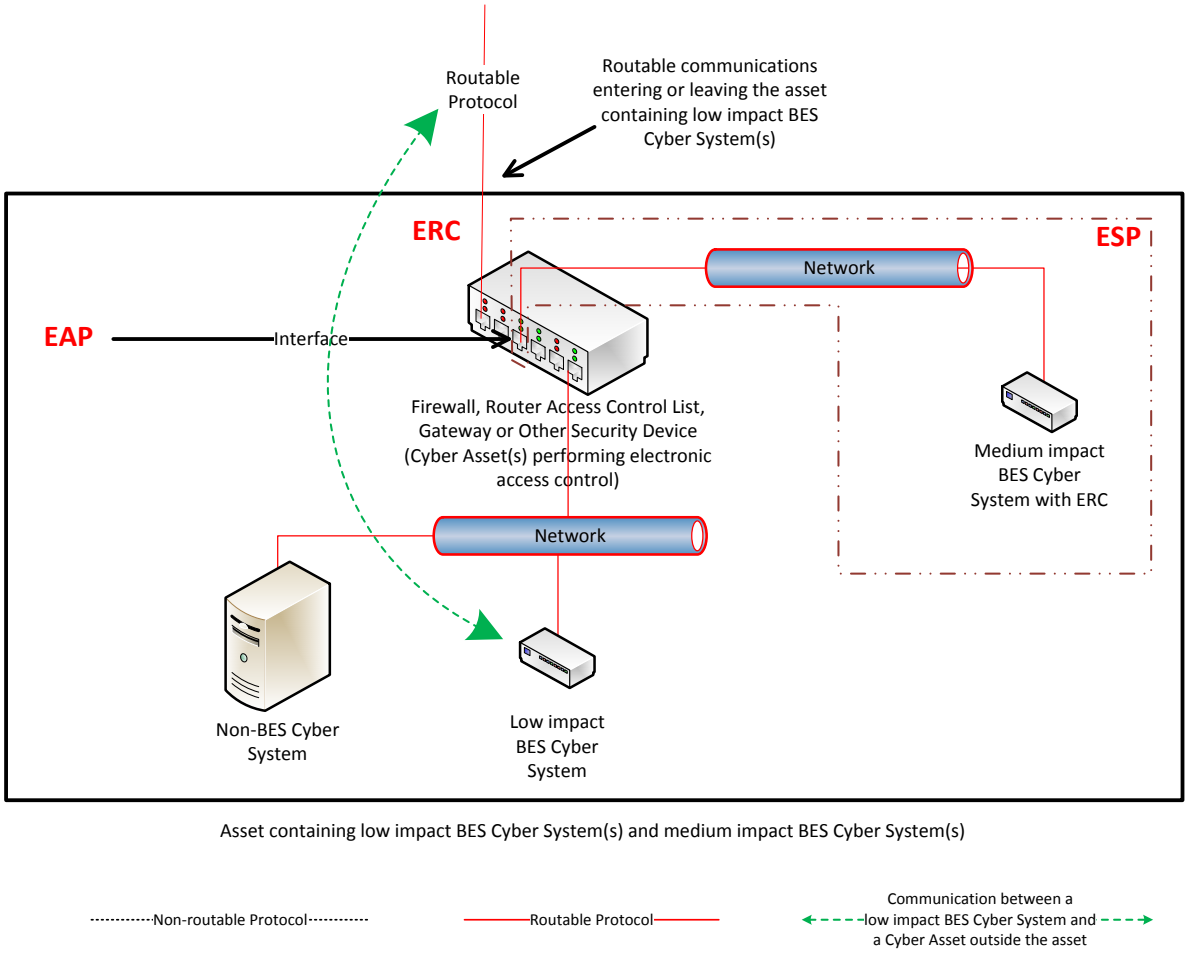
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device ~~connection," LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication to or from the low impact BES Cyber System.~~ that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.

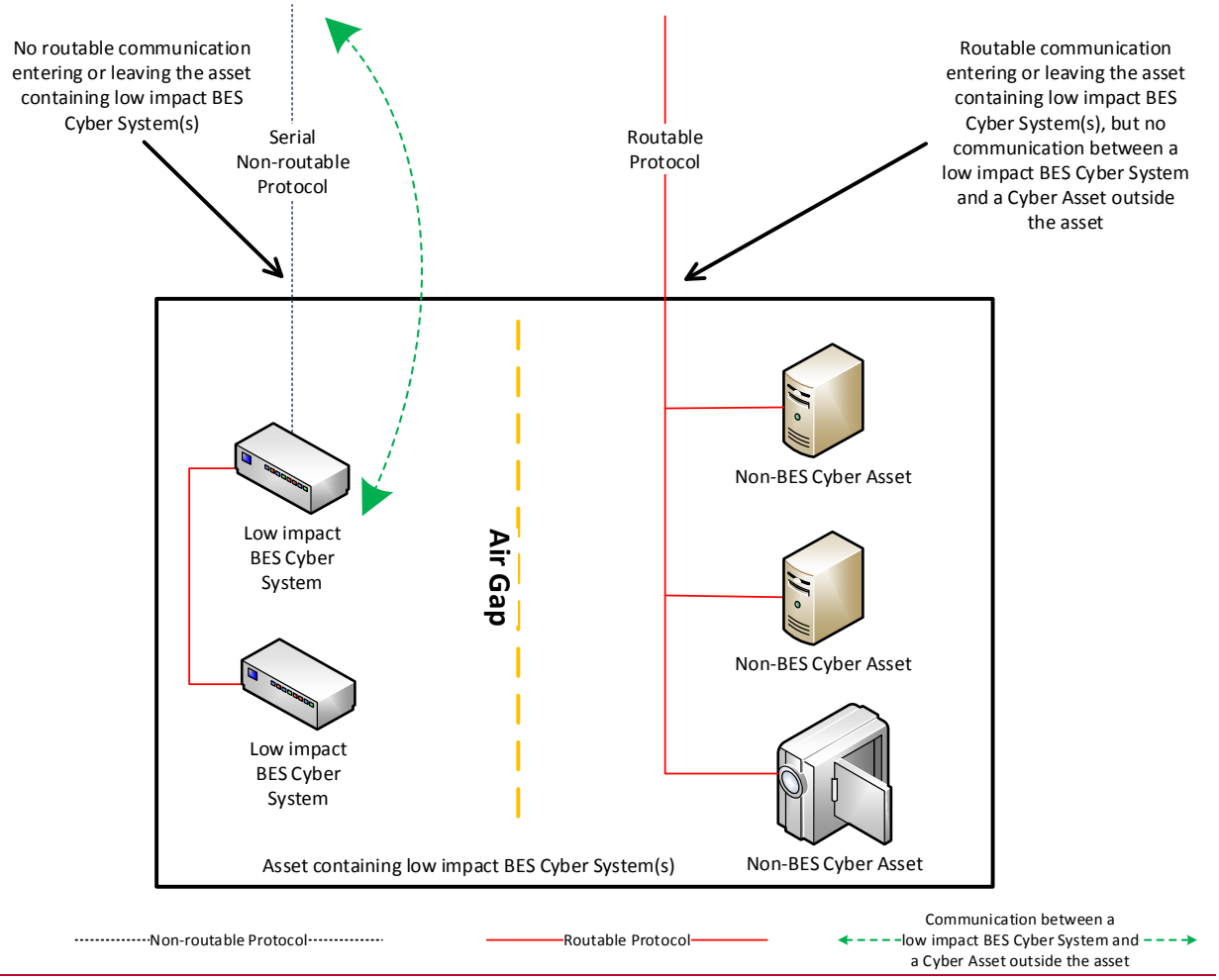


Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

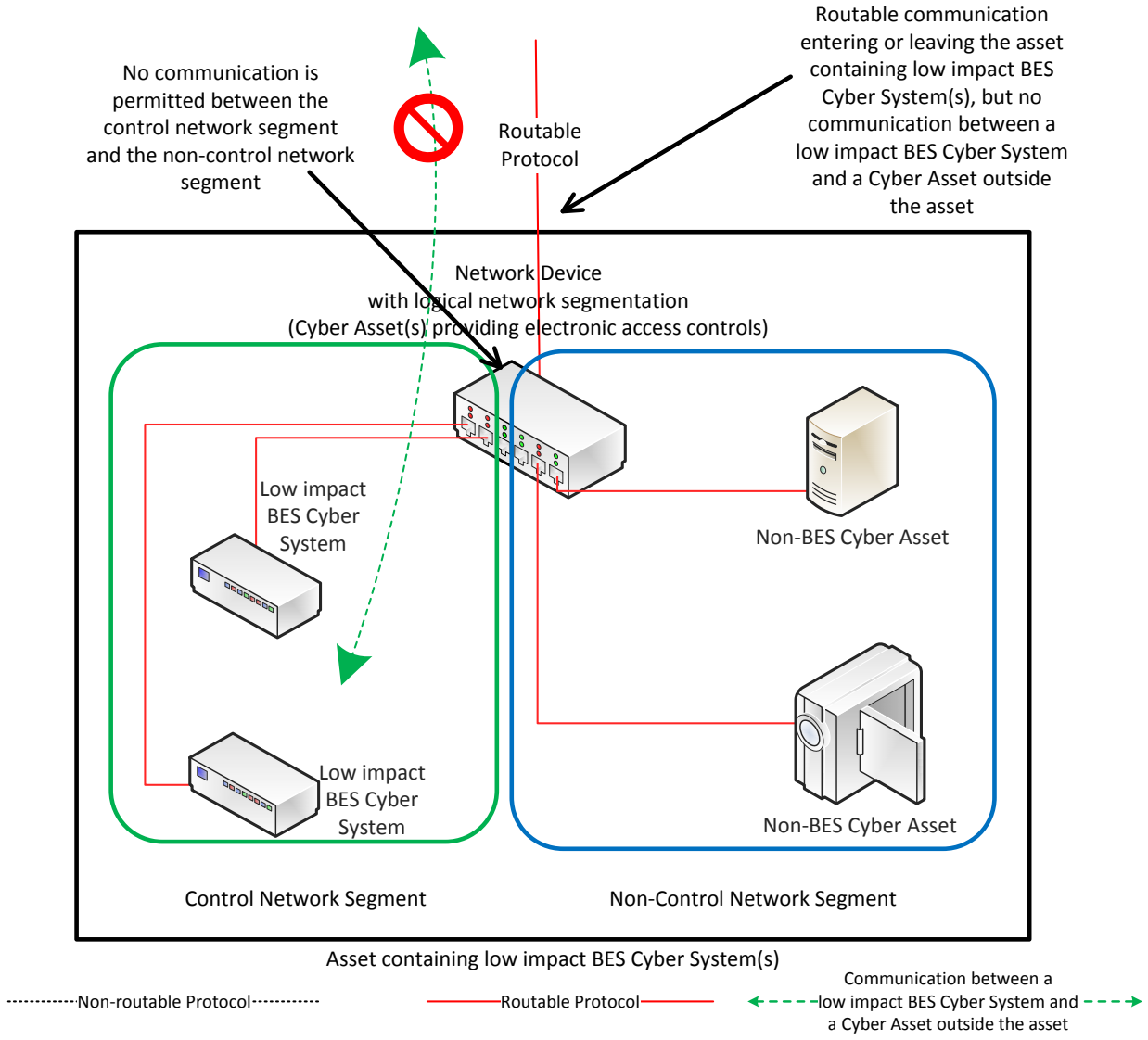
1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

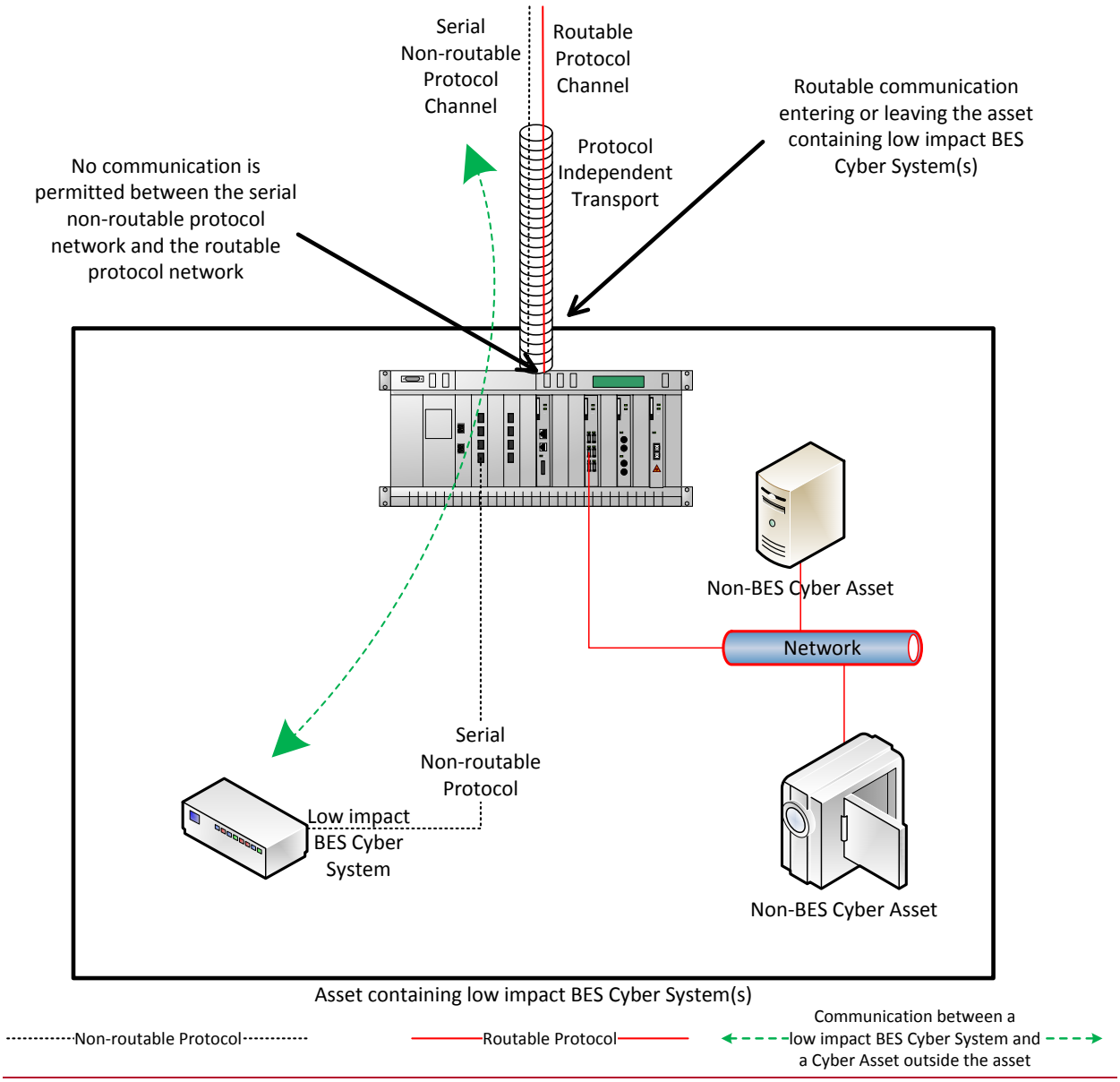
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

When identifying a LEAP, Responsible Entities are provided flexibility in the selection of the interface on a Cyber Asset that controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, the internal interface on a router that has implemented an access control list (ACL), or other security device. The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required to reside at the asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP per asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber Systems. Locating the Cyber Asset with multiple LEAPs at an external location with multiple assets containing low impact BES Cyber Systems "behind" it, however, should not allow uncontrolled access to assets containing low impact BES Cyber Systems sharing a Cyber Asset containing the LEAP(s).

In Reference Model 4, the communication flows through an IP/Serial converter. LERC is correctly identified in this Reference Model because the IP/Serial converter in this instance is doing nothing more than extending the communication between the low impact BES Cyber System and the Cyber Asset outside the asset containing the low impact BES Cyber System. In contrast, Reference Model 6 has placed a Cyber Asset that performs a complete break or interruption that does not allow the user or device data flow to directly communicate with the low impact BES Cyber System. The Cyber Asset in Reference Model 6 is preventing extending access to the low impact BES Cyber System from the Cyber Asset outside the asset containing the low impact BES Cyber System. The intent is that if the IP/Serial converter that is deployed only does a "pass-through" of the data flow communication, then that "pass-through" data flow communication is LERC and a LEAP is required. However, if that IP/Serial converter performs some type of authentication in the data flow at the asset containing the low impact BES Cyber System before the communication can be sent to the low impact BES Cyber System, then that type of IP/Serial converter implementation is not LERC.

A Cyber Asset that contains interface(s) that only perform the function of a LEAP does not meet the definition of Electronic Access Control or Monitoring System (EACMS) associated with medium or high impact BES Cyber Systems and is not subject to the requirements applicable to an EACMS. However, a Cyber Asset may contain some interfaces that function as a LEAP and other interfaces that function as an EAP for high or medium impact BES Cyber Systems. In this case, the Cyber Asset would also be subject to the requirements applicable to the EACMS associated with the medium or high impact BES Cyber Systems.

Examples of sufficient access controls may include:

- Any LERC for the asset passes through a LEAP with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g., IP addresses, ports, or services).
- As shown in Reference Model 1 below, the low impact BES Cyber System has a host-based firewall that is controlling the inbound and outbound access. In this

~~model, it is also possible that the host-based firewall could be on a non-BES Cyber Asset. The intent is that the host-based firewall controls the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in the business network.~~

- ~~As shown in Reference Model 5 below, a non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that the non-BES Cyber Asset has provided a "protocol break" so that access to the low impact BES Cyber System is only from the non-BES Cyber Asset that is located within the asset containing the low impact BES Cyber System.~~

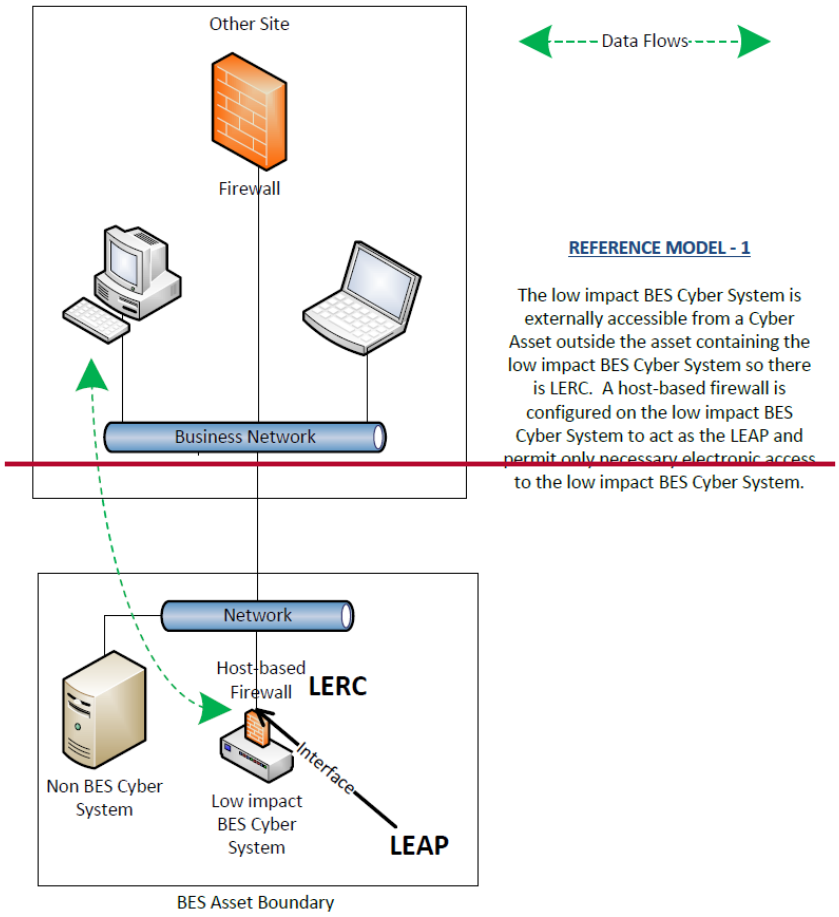
Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

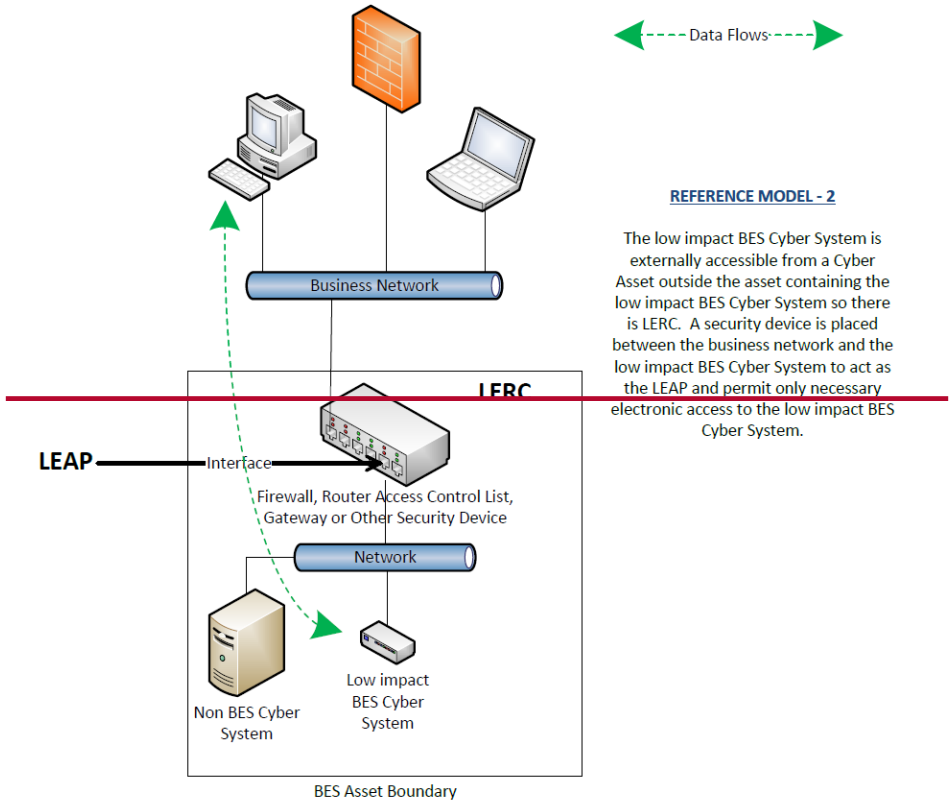
- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- ~~An asset has LERC due to a~~A low impact BES Cyber System ~~within it having~~has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- ~~In Reference Model 5, using just dual~~Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the ~~business~~external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security ~~device~~devices on ~~that~~the non-BES Cyber Asset.

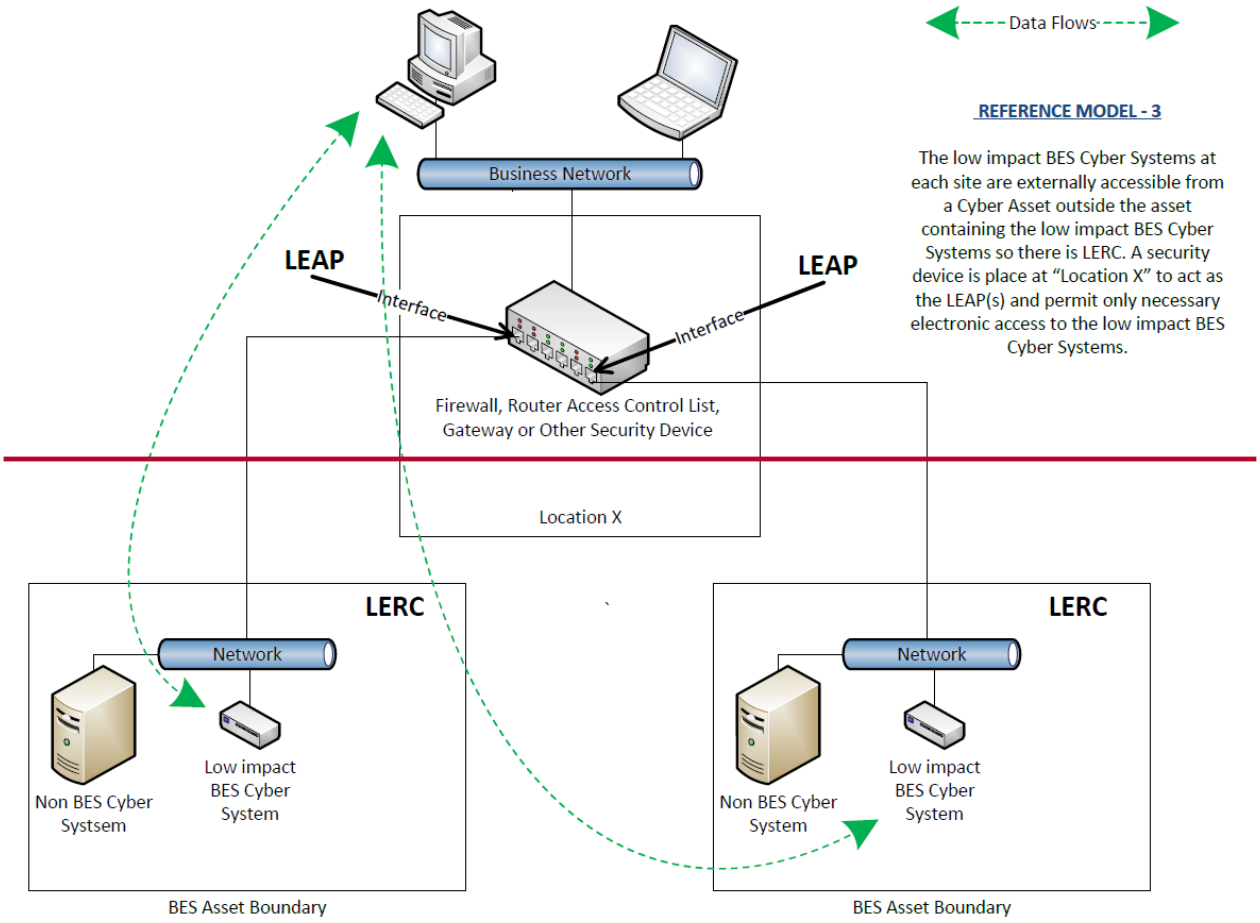
~~The following diagrams provide reference examples intended to illustrate how to determine whether there is LERC and for implementing a LEAP. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.~~

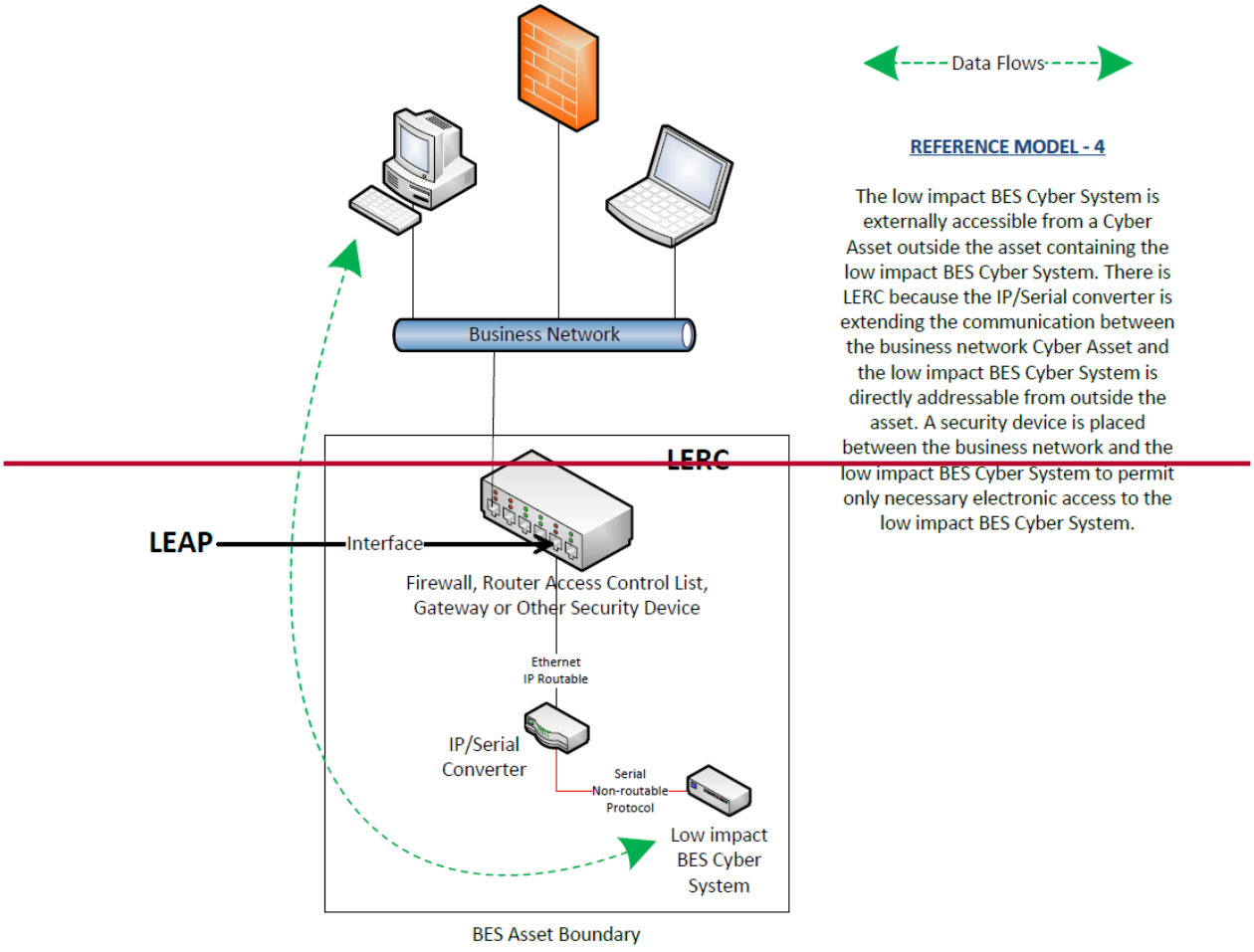


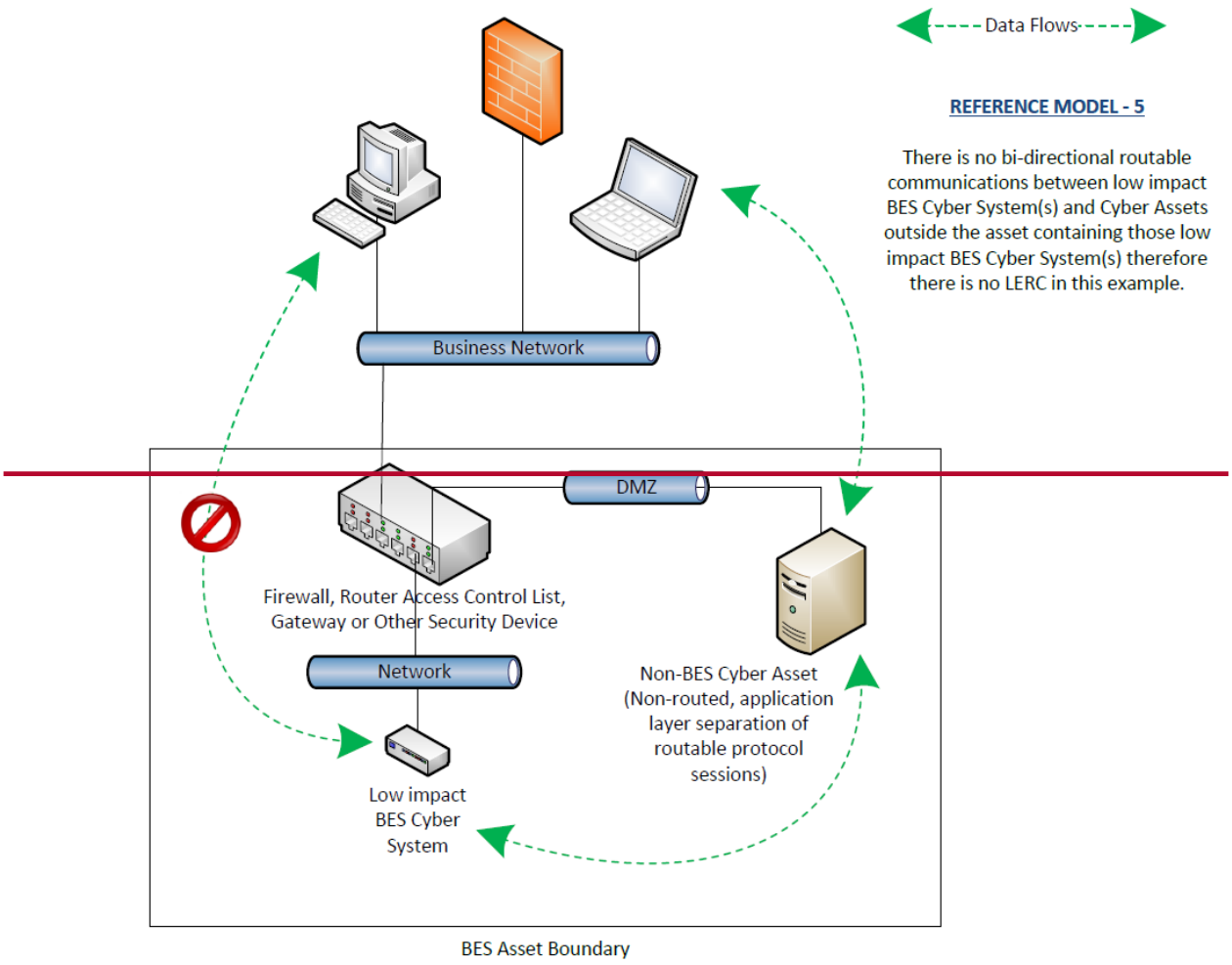
REFERENCE MODEL - 1

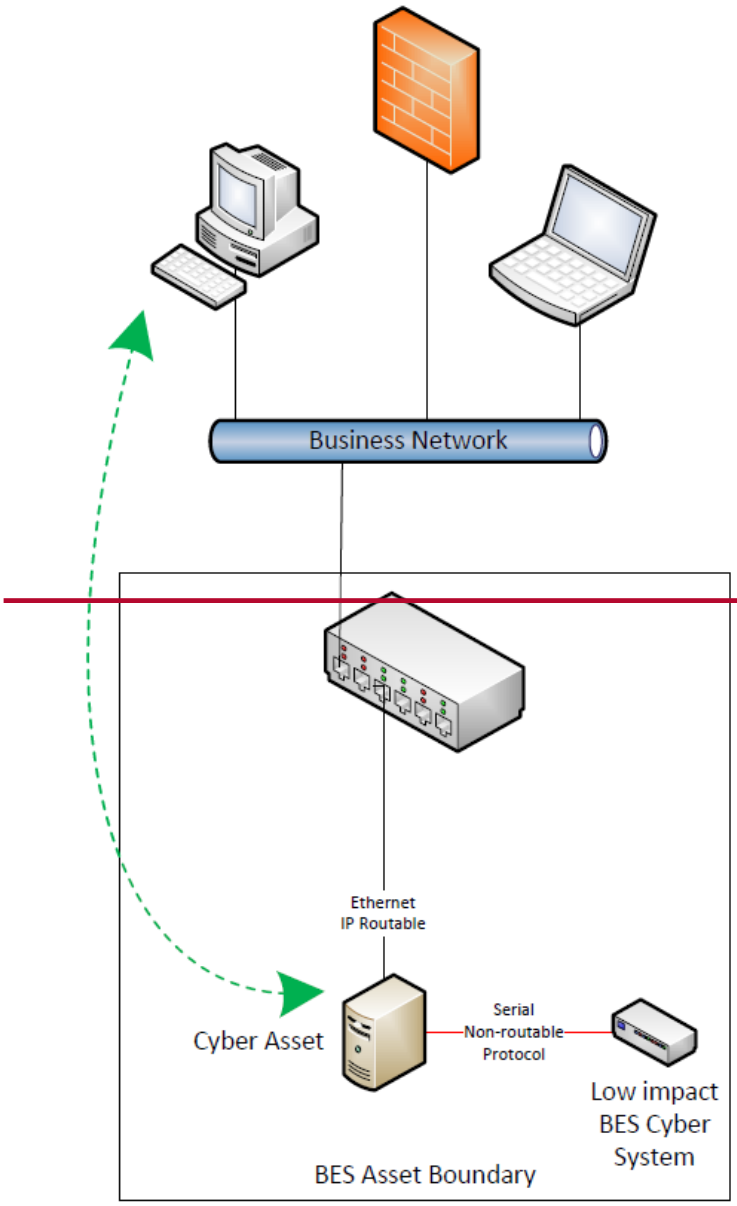
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A host-based firewall is configured on the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.


Data Flows
REFERENCE MODEL - 2
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.
Business Network
LERC
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary


Data Flows
REFERENCE MODEL - 3
The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is place at "Location X" to act as the LEAP(s) and permit only necessary electronic access to the low impact BES Cyber Systems.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Location X
LERC
Network
Non BES Cyber Systsem
Low impact BES Cyber System
BES Asset Boundary
LERC
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary


Data Flows
REFERENCE MODEL - 4
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.
Business Network
LERC
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Ethernet IP Routable
IP/Serial Converter
Serial Non-routable Protocol
Low impact BES Cyber System
BES Asset Boundary

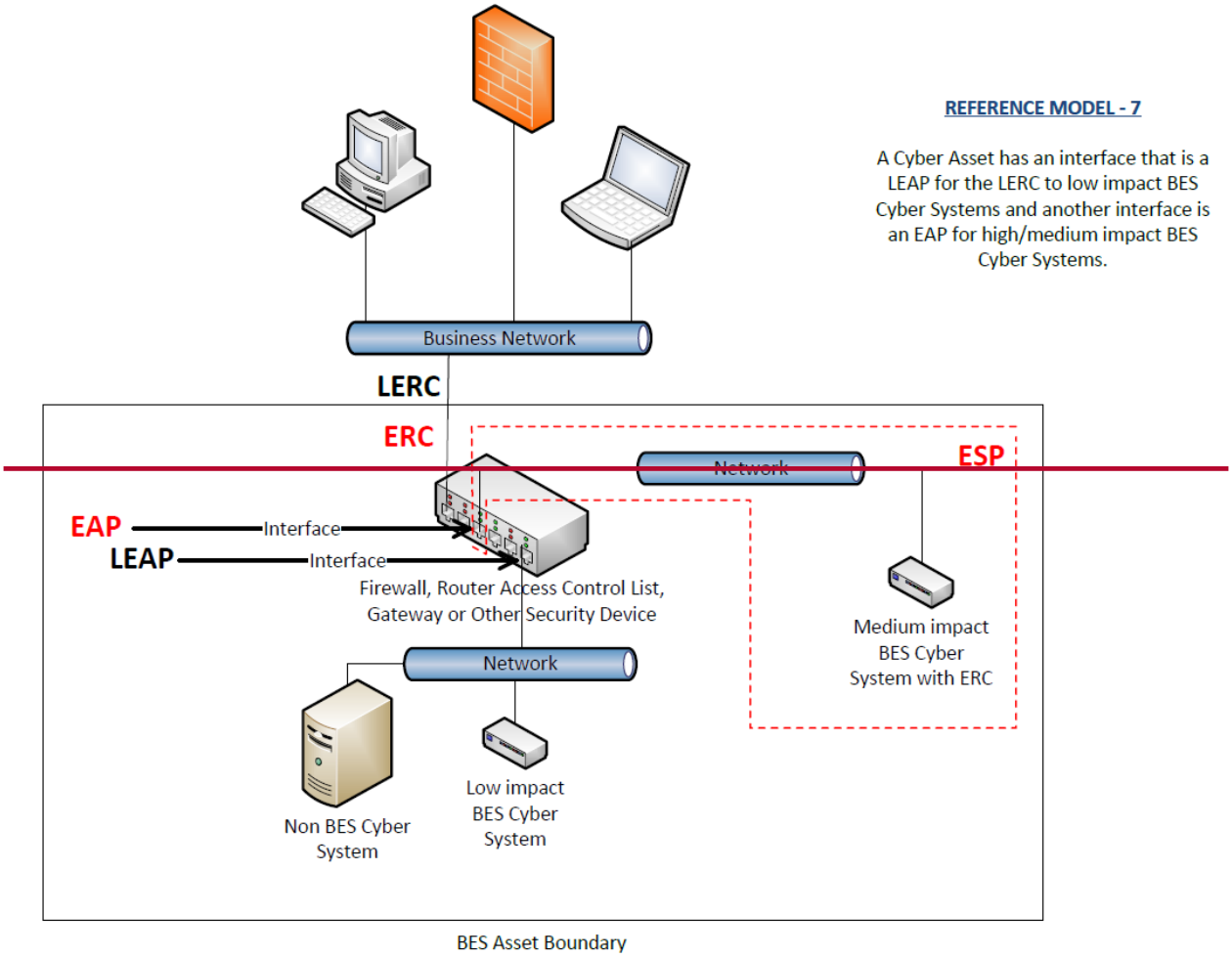

Data Flows
REFERENCE MODEL - 5
There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.
Business Network
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset (Non-routed, application layer separation of routable protocol sessions)
Low impact BES Cyber System
BES Asset Boundary



Data Flows

REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.



Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber ~~Systems,~~System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident

counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties

other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Malicious Code Risk Mitigation

The terms "mitigate", "mitigating", and "mitigation" are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that

can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-~~6~~7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-~~6~~7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:
During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:
One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:
In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber ~~Systems.~~System(s). The cyber security plan(s) covers ~~four~~five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; ~~and~~ (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber ~~Systems.~~System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber ~~Systems~~System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):
Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition

and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

Rationale for Section 5 of Attachment 1 (Requirement R2):
Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Rationale for Requirement R3:
The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

Exhibit B

Proposed Definitions for *Glossary of Terms Used in NERC Reliability Standards*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed Definitions of: "Transient Cyber Asset" (TCA) and "Removable Media"

Term: "Transient Cyber Asset" (TCA)

Revised Definition:

A Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Redline Definition:

A Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Currently Approved Definition of "Transient Cyber Asset" (TCA):

A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Term: "Removable Media"

Revised Definition:

Storage media that:

1. are not Cyber Assets,
2. are capable of transferring executable code,
3. can be used to store, copy, move, or access data, and
4. are directly connected for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Redline Definition:

Storage media that:

1. are not Cyber Assets,
2. are capable of transferring executable code,
3. can be used to store, copy, move, or access data, and
4. are directly connected for 30 consecutive calendar days or less to a:
   - BES Cyber Asset, ~~a~~
   - network within an Electronic Security Perimeter (ESP)~~,~~ containing high or medium impact BES Cyber Systems, or ~~a~~
   - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Currently Approved Definition of "Removable Media":

Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Exhibit E

Consideration of Issues and Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2016-02 Modifications to CIP Standards

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
After consideration of the comments received on this issue, we conclude that the adoption of controls for transient devices used at Low Impact BES Cyber Systems, including Low Impact Control Centers, will provide an important enhancement to the security posture of the bulk electric system by reinforcing the defense-in-depth nature of the CIP Reliability Standards at all impact levels. Accordingly, we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.	FERC Order 822, Paragraph 32; issued January 21, 2016	The Project 2016-02 Standard Drafting Team (SDT) revised Attachment 1 of CIP-003-7 to mitigate the risk to the BES of malware propagation to low impact BES Cyber Systems from transient devices. Attachment 1 contains and outlines the required sections of a Responsible Entity's cyber security plan(s) for its low impact BES Cyber Systems per Requirement R2. Previously, cyber security plan(s) were required to address four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. In keeping with the stakeholder approved approach to incorporate all the requirements applicable to assets containing low impact BES Cyber Systems into one standard, the SDT expanded CIP-003-7 Attachment 1 to include a fifth area: "Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation". Requiring the Responsible Entity to develop and implement these plans will provide higher assurance against the propagation of malware from transient devices. The plan approach for TCAs and Removable Media is consistent with the existing requirement structure applicable to lows and accommodates the risk level of the assets. Additionally, the SDT revised the definitions of Transient Cyber Asset (TCA) and Removable Media. The revised definitions ensure the applicability of security controls, provide clarity, and accommodate the use of the terms for all impact levels: high,

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		medium and low. The revised definitions will allow entities to deploy one program to manage TCAs and Removable Media across multiple impact levels. The revised definition of a Transient Cyber Asset (TCA) is: A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. The revised definition of Removable Media is: Storage media that: 1. are not Cyber Assets, 2. are capable of transferring executable code,

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		3. can be used to store, copy, move, or access data, and 4. are directly connected for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Service Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • Protected Cyber Asset associated with high or medium impact BES Cyber Systems. Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. As proposed, Section 5 of Attachment 1 of CIP-003-7 mandates that entities have malware protection on Transient Cyber Assets (both entity and vendor-managed) and for Removable Media. The SDT determined that it was necessary to distinguish between the specific protections for: (i) Transient Cyber Assets managed by the Responsible Entity, (ii) Transient Cyber Assets managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media. For Transient Cyber Assets managed by the Responsible Entity, Section 5 requires Responsible Entities to use one or a combination of the following to mitigate the introduction of malicious code: antivirus software, application whitelisting, or some other method. The SDT recognizes that Responsible Entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices (i.e., manage in an

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		ongoing manner) while others have a checklist for transient devices prior to connecting them to a BES Cyber System (i.e., manage in an on-demand manner). The drafting team acknowledges both methods are effective and Section 5 permits either form of management. Because of the higher frequency in which these entity-managed devices are used, the controls required for these devices are more specific. For Transient Cyber Assets managed by a party other than the Responsible Entity, Section 5 requires the Responsible Entity to review and verify the malware mitigation mechanism(s) used by the third party prior to connecting the Transient Cyber Asset (per Transient Cyber Asset capability). For Removable Media, Section 5 requires entities to employ methods to detect malicious code and mitigate the threat of detected malicious code prior to conecting to a low impact BES Cyber System.

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.	FERC Order 822, Paragraph 73; issued January 21, 2016	The Project 2016-02 Standard Drafting Team (SDT) resolved the ambiguity identified by the Commission surrounding the term "direct" within the definition of Low Impact External Routable Connectivity (LERC) by retiring the term and incorporating the LERC concepts within the requirement language. Retiring the LERC definition removes the dependency between the electronic access controls that may be in place and having those controls determine whether LERC exists or not. The SDT determined that indirect access, regardless of what kind of security break is in place causing it to be indirect, is another form of electronic access control that is intended to meet the same security objective. The SDT determined that the requirements should address the electronic access controls rather than having some controls implied through the definition. In changing the approach, the SDT avoids overemphasis on identifying LERC and focuses emphasis on the security objective in the requirements. Therefore, for those assets containing low impact BES Cyber Systems as identified in CIP-002, the SDT changed the language in Attachment 1, Section 3.1 from requiring a Low Impact Electronic Access Point (LEAP) to requiring that electronic access controls be implemented to meet the security objective of permitting "only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s); ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and,

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)." Additionally, the SDT updated and incorporated the exclusion language from the approved LERC definition into the requirement language and expanded the Guidelines and Technical Basis with numerous examples of electronic access control concepts that accomplish the defined security objective. Given the proposed retirement of LERC and the proposed modifications in Reliability CIP-003-7, there is no longer a need for the NERC Glossary term Low Impact BES Cyber System Electronic Access Point (LEAP). Consequently, the SDT proposed the term's retirement.

Exhibit F

Analysis of Violation Risk Factors and Violation Severity Levels

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of the violation risk factors (VRFs) and violation severity levels (VSLs) for Requirements R1 and R2 in proposed NERC Reliability Standard CIP-003-7 - Cyber Security — Security Management Controls. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-003-7, Requirement R2	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Lower was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements for low impact BES Cyber Systems. The purpose of the plan is for entities to develop an approach involving multiple procedures to address a broad subject matter. Using a plan, Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems.
FERC VRF G1 Discussion Guideline 1 - Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2 - Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement a documented cyber security plan that contains certain sections specified in Attachment 1. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security plan, the VRF is reflective of the plan as a whole. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain low impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3 - Consistency among Reliability Standards	This requirement maps from CIP-003-6, Requirement R2, which has an approved VRF of Lower; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Failure to properly implement the cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state

VRF Justifications for CIP-003-7, Requirement R2	
Proposed VRF	**Lower**
Guideline 4 - Consistency with NERC Definitions of VRFs	or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion Guideline 5 - Treatment of Requirements that Co-mingle More than One Obligation	The cyber security plan requirement encompasses a number of subject matter areas for low impact BES Cyber Systems. The VRF is identified at the risk level represented by all of the plan areas in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.

VSLs for CIP-003-7, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES

VSLs for CIP-003-7, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the six topics required by R1. (R1.2)	impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the six topics required by R1. (R1.2)	impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the six topics required by R1. (R1.2)	Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more

VSLs for CIP-003-7, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
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 BES Cyber Systems 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. (R1.2) 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 BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems 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. (R1.2) 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 BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) 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 BES Cyber Systems 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. (R1.2)	of the six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

VSL Justifications for CIP-003-7, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved Requirement R1, CIP-003-6. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-003-7, Requirement R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security policy(s) but fails to include one or more of the required sections of Attachment 1. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The action of the requirement is to document cyber security policy(s). Implementation of the cyber security policy(s) is demonstrated through performance of Requirement R2. There is no documentation and implementation interdependence within Requirement R1.

VSLs for CIP-003-7, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented its cyber security	The Responsible Entity documented its cyber security	The Responsible Entity documented the physical access	The Responsible Entity failed to document and implement one

VSLs for CIP-003-7, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber	plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR	controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36	or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

VSLs for CIP-003-7, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing	calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR	

VSLs for CIP-003-7, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
	low impact BES Cyber Systems, but failed to document the 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	

VSLs for CIP-003-7, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
	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 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)		

VSL Justifications for CIP-003-7, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved Requirement R2, CIP-003-6. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-003-7, Requirement R2	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security plan(s) but fails to address one or more of the required sections of Attachment 1. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The action of the requirement is to implement documented cyber security plan(s). Documentation of the plan(s) is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the plan in this case; as such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity implemented all the required elements of the plan. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

Exhibit G

Summary of Development History and Record of Development

Summary of Development History

Summary of Development History

The development record for proposed Reliability Standard CIP-003-7 is summarized below.

I. Overview of the Standard Drafting Team

When evaluating a proposed Reliability Standard, the Commission is expected to give "due weight" to the technical expertise of the ERO.[1] The technical expertise of the ERO is derived from the standard drafting team selected to lead each project in accordance with Section 4.3 of the NERC Standards Process Manual.[2] For this project, the standard drafting team consisted of industry experts, all with a diverse set of experiences. A roster of the Standard Drafting team ("SDT") members is included in **Exhibit H**.

II. Standard Development History

A. Standard Authorization Request Development

Project 2016-02 – Modifications to CIP Standards was initiated to address Commission directives in Order No. 822.[3] In Order No. 822, the Commission directed NERC to: (1) modify the definition of Low Impact External Routable Communication ("LERC") by removing the word "direct" to clarify the electronic access controls for Low Impact BES Cyber System(s); and (2) develop certain modifications to the CIP standards to provide mandatory protection for transient devices used at low impact BES Cyber Systems.[4] The Commission directed NERC to file modifications to the LERC definition within one year of the effective date of Order No. 822.

---

1 Section 215(d)(2) of the Federal Power Act; 16 U.S.C. §824(d)(2) (2012).

2 The NERC *Standard Processes Manual* is available at http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf.

3 Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards* 154 FERC ¶ 61,037, 81 Fed. Reg. 4177 (2016).

4 *Id*.

The Standards Authorization Request ("SAR") for Project 2016-02 was initially posted on March 23, 2016 for a 30-day informal comment period. The SAR was modified in response to industry feedback to include certain additional items and was posted for a 30-day informal comment period from June 1, 2016 through June 30, 2016. The SAR was accepted by the Standards Committee on July 20, 2016.

B. First Posting - Comment Period, Initial Ballots and Non-binding Poll

Given the filing deadline associated with the LERC directive, NERC prioritized development of revisions to address that directive. On July 21, 2016, NERC posted the initial draft of proposed Reliability Standard CIP-003-7 addressing only the LERC directive for a 45-day comment period, the associated Implementation Plan , and a revised definition of LERC were posted for a 45-day formal comment period from July 21, 2016 through September 6, 2016, with parallel Initial Ballots and a Non-binding Poll for the Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") held during the last 10 days of the comment period from August 26, 2016 through September 6, 2016. The Initial Ballot for CIP-003-7 received 85.00% quorum, and 41.54% approval. The Initial Ballot for the proposed Implementation Plan received 84.37% quorum, and 41.77% approval. The Initial Ballot for the LERC and its definitions received 84.62% quorum, and 30.63% approval. The Non-binding Poll for the associated VRFs and VSLs received 83.18% quorum and 37.73% of supportive opinions. There were 76 sets of responses, including comments from approximately 169 different individuals and approximately 126 companies, representing 9 of the 10 industry segments.[5]

[5] NERC, *Consideration of Comments*, Project 2016-02 Modifications to CIP Standards, (October 21, 2016), *available at* http://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/2016-02_CIP_Consideration_of_Comments_10212016.pdf.

C. Second Posting- Comment Period, Additional Ballots and Non-binding Poll

Proposed Reliability Standard CIP-003-7 and the associated Implementation Plan were posted for another 45-day formal comment period from October 21, 2016 through December 5, 2016, with parallel Additional Ballots and a Non-binding Poll held during the last 10 days of the comment period from November 23, 2016 through December 5, 2016.[6] The second draft of CIP-003-7 also only addressed the LERC directive. The Additional Ballot for CIP-003-7 reached quorum at 76.40% of the ballot pool, and received 85.56% approval. The Additional Ballot for the proposed Implementation Plan reached quorum at 76.63% of the ballot pool, and received 75.54% approval. The related Non-Binding Poll for the associated VRFs and VSLs reached quorum 75.00% of the ballot pool, with 82.47% of supportive opinions. There were 61 sets of responses, including comments from approximately 136 different individuals and approximately 108 companies, representing 9 of the 10 industry segments.[7]

D. Final Ballot

Proposed Reliability Standard CIP-003-7, addressing only the LERC directive, and the associated Implementation Plan were posted for a 10-final ballot period from December 9, 2016 through December 19, 2016. The ballot for proposed Reliability Standard CIP-003-7 reached quorum at 82.89% of the ballot pool, and the standard received sufficient affirmative votes for approval, receiving support from 87.95% of the voters. The ballot for the proposed Implementation Plan reached quorum at 83.14% of the ballot pool, and the standard received sufficient affirmative votes for approval, receiving support from 83.03% of the voters.

---

[6] During the development of the second draft of CIP-003-7, the SDT also began to develop language in response to the transient electronic devices directive. On November 1, 2016, NERC posted draft revisions to CIP-003-7 to address the transient electronic device directive for a 17- day informal comment period.

[7] NERC, *Consideration of Comments*, Project 2016-02 Modifications to CIP Standards, (December 2016), *available at* http://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/2016-02_CIP-003-7_Consideration_of_Comments_12092016.pdf.

E. Third Posting - Comment Period, Initial Ballots and Non-binding Poll

During the second posting of CIP-003-7, the standard drafting team also began to develop language in response to the transient electronic device directive. On November 1, 2016, NERC posted draft revisions to CIP-003-7 to also address the transient electronic device directive for a 17-day informal comment period. On December 12, 2016, after considering comments received on the informal posting, NERC posted a third draft of CIP-003-7[8] that included the modifications to address the LERC directive, which had already received the requisite stakeholder approval, as well as modifications to address the transient electronic device directive for a 45-day comment period and ballot, with parallel Additional Ballots and a Non-binding Poll held during the last 10 days of the comment period from January 16, 2017 through January 25, 2017.[9] The ballot for proposed Reliability Standard CIP-003-7 received 77.81% quorum, and 81.30% approval. The ballot for the proposed Implementation Plan received 76.71% quorum, and 87.87% approval. The ballot for the proposed revisions to the definition to Transient Cyber Assets (TCA) definition received 77.26% quorum, and 86.75% approval. The ballot for the proposed Removable Media definition received 76.71% quorum, and 86.47% approval. The Non-binding Poll for this draft of CIP-003-7 received 76.73% quorum and 79.74% of supportive opinions. There were 50 sets of responses, including comments from approximately 136 different individuals and approximately 110 companies, representing 9 of the 10 industry segments.[10]

---

[8] During development, the third draft of CIP-003-7 was balloted as CIP-003-7(i). Romanette (i) was included in the version numbering to differentiate it from the earlier ballot of CIP-003-7 that only addressed the LERC directive.

[9] The Non-binding Poll was extended an additional day to January 26, 2017 to reach quorum.

[10] NERC, *Consideration of Comments*, Project 2016-02 Modifications to CIP Standards, (January 30, 2017), *available at* http://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/2016-02_CIP-003-7i_TCA_Comment_Report_01302017.pdf.

F. Final Ballot

The draft of proposed Reliability Standard CIP-003-7 that included both the LERC directive and transient electronic device modifications, the associated Implementation Plan, and the proposed revised definitions TCA and Removable Media were posted for a 10-final ballot period from January 30, 2017 through February 8, 2017. The ballot for proposed Reliability Standard CIP-003-7 reached quorum at 86.58% of the ballot pool, and the standard received sufficient affirmative votes for approval, receiving support from 78.55% of the voters. The ballot for the proposed Implementation Plan reached quorum at 85.48% of the ballot pool, and the standard received sufficient affirmative votes for approval, receiving support from 86.00% of the voters. The ballot for the proposed TCA definition reached quorum at 86.03% of the ballot pool, and the standard received sufficient affirmative votes for approval, receiving support from 85.81% of the voters. The ballot for the proposed Removable Media definition reached quorum at 85.48% of the ballot pool, and the standard received sufficient affirmative votes for approval, receiving support from 85.54% of the voters.

G. Board of Trustees Adoption

Proposed Reliability Standard CIP-003-7 was adopted by the NERC Board of Trustees on February 9, 2017.[11]

[11] NERC, *Board of Trustees Agenda Package*, Agenda Item 4c (Project 2016-02 Modifications to CIP Standards (CIP-003-7)), *available at* http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Board_February_9_2017_Meeting_Agenda_Package_v3.pdf.

Complete Record of Development

Project 2016-02 Modifications to CIP Standards

Related Files

Status
10-day final ballots for the following concluded **8 p.m. Eastern, Wednesday, February 8, 2017**:

1. CIP-003-7(i) - Cyber Security – Security Management Controls

2. CIP-003-7(i) Implementation Plan

3. Transient Cyber Asset (TCA) - Proposed revised definition

4. Removable Media - Proposed revised definition

Final ballots for **CIP-003-7 - Cyber Security – Security Management Controls** and the **CIP-003-7 Implementation Plan** concluded **8 p.m. Eastern, Monday, December 19, 2016**.

All voting results can be accessed via the links below. The standard, implementation plans, and definitions will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Background
The Version 5 Transition Advisory Group (V5 TAG) transferred issues to the Version 5 Standard Drafting Team (SDT) that were identified during the industry transition to implementation of the Version 5 CIP Standards. Specifically, the issues that the SDT will address are:

- Cyber Asset and BES Cyber Asset Definitions
- Network and Externally Accessible Devices
- Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations
- Virtualization

On January 21, 2016, FERC issued Order No. 822 Revised Critical Infrastructure Protection Reliability Standards. In this order, FERC approved revisions to version 5 of the CIP standards and also directed that NERC address each of the Order 822 directives by developing modifications to requirements in CIP standards and the definition of Low Impact External Routable Connectivity (LERC), or the SDT shall develop an equally efficient and effective alternative. To address concerns identified in Order 822, the Commission directed the following:

- Develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability.
- Develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).
- Develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule, to the LERC definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

Standard(s) Affected – CIP-002-5.1, CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, CIP-011-2

Purpose/Industry Need
The SDT will modify the CIP family of standards (or develop an equally efficient and effective alternative) to:

- Address issues identified by the CIP V5 TAG;
- Address FERC directives contained in Order 822; and
- Address requests for interpretations as directed by the NERC Standards

Draft	Actions	Dates	Results	Consideration of Comments
Final Draft CIP-003-7(i) Clean **(83)** | Redline to Last Posted **(84)** Implementation Plan Clean **(85)** | Redline to Last Posted **(86)** Definition of Terms Used in Standards (TCA and Removable Media) Clean **(87)** | Redline to Last Posted **(88)**	Final Ballots Info **(89)** Vote	01/30/17 - 02/08/17	Ballot Results CIP-003-7(i) **(90)** Implementation Plan **(91)** TCA Definition **(92)** Removable Media Definition **(93)**	
Draft 1 **CIP-003-7(i)** Clean **(65)** | Redline to Last Approved **(66)** | Redline to CIP-003-7 **(67)** Implementation Plan **(68)** Definition of Terms Used in Standards (TCA and Removable Media) **(69)**	Initial Ballots and Non-binding Poll Updated Info **(73)** Info **(74)** Vote	01/16/17 - 01/25/17 (The Non-binding Poll was extended to 01/26/17 to meet quorum)	Ballot Results CIP-003-7(i) **(75)** Implementation Plan **(76)** TCA Definition **(77)** Removable Media Definition **(78)** Non-binding Poll **(79)**	

Supporting Documents Unofficial Comment Form (Word) **(70)** VRF/VSL Justification **(71)** Consideration of Issues and Directives **(72)** **CIP-003-7(i)** **Draft Reliability Standard Audit Worksheet (RSAW)** Updated Clean | Redline to CIP-003-6	Comment Period Info **(80)** Submit Comments	12/12/16 - 01/25/17	Comments Received **(81)**	Consideration of Comments **(82)**
	Join Ballot Pools The existing CIP-003-7 (LERC) ballot pool was used for all of the ballots associated with this portion of the project. The ballot pools have been re-opened to allow stakeholders to join if they are not existing members.	12/12/16 - 01/10/17		
	Updated Info Send RSAW feedback to: RSAWfeedback@nerc.net	12/27/16 - 01/25/17 Updated RSAW posted January 20, 2017		
Final Draft **CIP-003-7** Clean **(58)** | Redline to Last Posted **(59)** Implementation Plan Clean **(60)** | Redline to Last Posted **(61)**	Final Ballots Info **(62)** Vote	12/09/16 - 12/19/16	Ballot Results CIP-003-7 **(63)** Implementation Plan **(64)**	
CIP-003-TCA Clean **(49)** | Redline to CIP-003-6 **(50)** TCA Implementation Plan **(51)** **Supporting Documents** Unofficial Comment Form (Word) **(52)** TCA Consideration of Issues and Directives **(53)** TCA VRF and VSL Justification **(54)** TCA Definition **(55)**	Informal Comment Period Info **(56)** Submit Comments	11/01/16 - 11/18/16	Comments Received **(57)**	
Draft 2 **CIP-003-7** Clean **(31)** | Redline to Last Posted **(32)** | Redline to Last Approved **(33)** Implementation Plan Clean **(34)** | Redline to Last Posted **(35)** **Supporting Documents** Unofficial Comment Form (Word) **(36)** VRF and VSL Justification Clean **(37)** | Redline to Last Posted **(38)** Consideration of Issues and Directives Clean **(39)** | Redline to Last Posted **(40)**	Additional Ballots and Non-binding Poll Updated Info **(41)** Info **(42)** Vote	11/23/16 - 12/05/16	Ballot Results CIP-003-7 **(42)** Implementation Plan **(44)** Non-binding Poll **(45)**	
	Comment Period Info **(46)** Submit Comments	10/21/16 - 12/05/16	Comments Received **(47)**	Consideration of Comments **(48)**
CIP-003-7 **Draft Reliability Standard Audit Worksheet (RSAW)** Clean | Redline	Info Send RSAW feedback to: RSAWfeedback@nerc.net	11/04/16 - 12/05/16		

Draft 1 **CIP-003-7** Clean **(14)** | Redline to Last Approved **(15)** **Definition of Term(s) Used in Standards** Clean **(16)** | Redline **(17)** Implementation Plan **(18)** **Supporting Documents** Unofficial Comment Form (Word) **(19)** VRF and VSL Justification **(20)** Consideration of Issues and Directives **(21)**	Initial Ballots and Non-binding Poll Updated Info **(22)** Info **(23)** Vote	08/26/16 - 09/06/16	Ballot Results CIP-003-7 **(24)** Implementation Plan **(25)** LERC and its Definition **(26)** Non-binding Poll **(27)**	
	Comment Period Info **(28)** Vote	07/21/16 - 09/06/16	Comments Received **(29)**	Consideration of Comments **(30)**
	Join Ballot Pools	07/21/16 - 08/19/16		
Draft CIP-003-7 RSAW Clean | Redline	Info Send RSAW Feedback to: RSAWfeedback@nerc.net	08/10/16 - 09/06/16		
The Standards Committee accepted the Standards Authorization Request on July 20, 2016				
Standards Authorization Request Clean **(8)** | Redline to Last Posted **(9)** **Supporting Materials** Unofficial Comment Form **(10)** CIP Version 5 Transition Advisory Group Issues for Consideration **(11)**	Comment Period Info **(12)** Submit Comments	06/01/16 - 06/30/16	Comments Received **(13)**	
Standards Authorization Request **(3)** **Supporting Materials** Unofficial Comment Form (Word) **(4)** CIP Version 5 Transition Advisory Group Issues for Consideration **(5)**	Comment Period Info **(6)** Submit Comments	03/23/16 - 04/21/16	Comments Received **(7)**	
Supplemental Standard Drafting Team Nominations **Supporting Materials** Unofficial Nomination Form (Word) **(1)**	Nomination Period Info **(2)** Submit Nominations	03/10/16 - 03/23/16		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2016-02 Modifications to CIP Standards

Supplemental Nomination Period

Nominations for additional standard drafting team (SDT) members are being solicited for **Project 2016-02 Modifications to CIP Standards**. Use the electronic form to submit nominations by **8 p.m. Eastern, Wednesday, March 23, 2016.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Documents and information about this project are available on the Project 2016-02 Modifications to CIP Standards page. If you have questions, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

Background

This solicitation for nominations is to supplement the existing Project 2016-02 Modifications to CIP Standards SDT that is continuing to address the work in the Project 2016-02 Modifications to CIP Standards Authorization Request (SAR). NERC is seeking individuals from the United States and Canada who possess experience in one or more of the following areas:

- Operations technology
- Communication networks
- Virtualization
- Protection of transient electronic devices
- Network and externally accessible devices
- Cyber Asset and BES Cyber Asset definitions
- Transmission Owner (TO) Control Centers
- Critical Infrastructure Protection ("CIP") family of Reliability Standards

The time commitment for Project 2016-02 is expected to be significant. Participants should anticipate an average workload of 20 hours per week devoted to the drafting team efforts. In-person meetings will occur typically for 2 ½ - 3 days most months (not including travel time) and meetings will take place in different parts of North America. When not meeting in person, regularly scheduled

conference calls will be used to conduct drafting team work. Outside the scheduled meetings, individuals or subgroups will have additional preparation and support work such as researching and developing proposed concepts, reviewing proposals, compiling comments and drafting responses, etc. Lastly, outreach is an important component of this drafting team's effort. Members of the team are expected to interact with other stakeholders during the revision development process.

Name:	
Organization:	
Address:	
Telephone:	
E-mail:	

Please briefly describe your experience and qualifications to serve on the requested Standard Drafting Team (Bio):

If you are currently a member of any NERC drafting team, please list each team here:

☐ Not currently on any active SAR or standard drafting team.

☐ Currently a member of the following SAR or standard drafting team(s):

If you previously worked on any NERC drafting team please identify the team(s):

☐ No prior NERC SAR or standard drafting team.

☐ Prior experience on the following team(s):

Select each NERC Region in which you have experience relevant to the Project for which you are volunteering:

☐ FRCC	☐ RF	☐ Texas RE
☐ MRO	☐ SERC	☐ WECC
☐ NPCC	☐ SPP RE	☐ NA – Not Applicable

Select each Industry Segment that you represent:

☐	1 — Transmission Owners

☐	2 — RTOs, ISOs
☐	3 — Load-serving Entities
☐	4 — Transmission-dependent Utilities
☐	5 — Electric Generators
☐	6 — Electricity Brokers, Aggregators, and Marketers
☐	7 — Large Electricity End Users
☐	8 — Small Electricity End Users
☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
☐	10 — Regional Reliability Organizations and Regional Entities
☐	NA – Not Applicable

Select each Function[1] in which you have current or prior expertise:

☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group:

Name:		Telephone:	
Organization:		E-mail:	
Name:		Telephone:	
Organization:		E-mail:	

[1] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

Provide the name and contact information of your immediate supervisor or a member of your management who can confirm your organization's willingness to support your active participation.			
Name:		Telephone:	
Title:		Email:	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Supplemental Nomination Period Open through March 23, 2016

Now Available

Nominations are being sought for additional standard drafting team (SDT) members through **8 p.m. Eastern, Wednesday, March 23, 2016**.

Use the electronic form to submit a nomination. If you experience any difficulties in using the electronic form, contact Wendy Muller. An unofficial Word version of the nomination form is posted on the Standard Drafting Team Vacancies page and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required.

The time commitment for this project is expected to be significant. Participants should anticipate an average workload of 20 hours per week devoted to the SDT efforts. In person meetings will occur typically for 2 ½ - 3 days most months (not including travel time) and meetings will take place in different parts of North America. When not meeting in person, regularly scheduled conference calls will be used to conduct drafting team work. Outside the scheduled meetings, individuals or subgroups will have additional preparation and support work such as researching and developing proposed concepts, reviewing proposals, compiling comments and drafting responses, etc. Lastly, outreach is an important component of this SDT's effort. Members of the team are expected to interact with other stakeholders during the revision development process.

See the project page and unofficial nomination form for more information.

Next Steps

The Standards Committee is expected to appoint members to the team in April 2016. Nominees will be notified shortly after they have been appointed.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326

404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard(s):	Modifications to CIP Standards		
Date Submitted:	March 9, 2016		
SAR Requester Information			
Name:	Stephen Crutchfield		
Organization:	NERC		
Telephone:	609-651-9455	E-mail:	Stephen.Crutchfield@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard		☒ Withdrawal of existing Standard	
☒ Revision to existing Standard		☐ Urgent Action	

SAR Information
Purpose (Describe what the standard action will achieve in support of Bulk Electric System reliability.):
The purpose of this project is to (1) consider the Version 5 Transition Advisory Group (V5TAG) issues identified in the *CIP V5 Issues for Standard Drafting Team Consideration* (V5TAG Transfer Document) and (2) address the Federal Energy Regulatory Commission (Commission) directives contained in Order 822. These revisions will increase reliability and security to the Bulk-Power System (BPS) by enhancing cyber protection of BPS facilities.
Industry Need (What is the industry problem this request is trying to solve?):
The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP version 5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by the existing standard drafting team (SDT) for the CIP Reliability Standards.

SAR Information

The V5 TAG developed the V5TAG Transfer Document to explain the issues and recommend that the SDT consider them in future development activity.

On January 21, 2016, the Commission issued Order No. 822 approving revisions to the CIP version 5 standards and also directing NERC to develop modifications to address:

- Protection of transient electronic devices used at low-impact BES Cyber Systems;
- Protections for communication network components between control centers; and
- Refinement of the Low Impact External Routable Connectivity (LERC) definition.

The Commission did not provide a date by which the modifications for transient devices or communication networks must be completed. For the LERC definition, however, the Commission directed that NERC submit the modification within one year of the effective date of Order No. 822 (March 31, 2017).

Brief Description (Provide a paragraph that describes the scope of this standard action.)

The proposed project will consider the issues raised by the V5TAG in the V5TAG Transfer Document and will address the Commission directives in Order No. 822 through modifications to the CIP standards. The work will include development of Violation Risk Factors, Violation Severity Levels, and an Implementation Plan for the modified standards and will meet the deadlines established by the Commission in Order No. 822.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

As stated above, the purpose of this project is to consider the V5TAG issues in the initial transfer document V5TAG Transfer Document and address the Commission directives contained in Order 822. For the directive on the LERC definition, the project is to respond within the deadline required in the order.

As noted above, the V5TAG identified specific issues with the CIP V5 standards. The V5TAG drafted the V5TAG Transfer Document to formally recommend that the SDT address these issues during standards development to consider whether modifications can be made to the standard language. As outlined in the V5TAG Transfer Document, the specific issues are as follows:

- Cyber Asset and BES Cyber Asset (BCA) Definitions – as foundational definitions within the CIP V5 standards, the understanding of Cyber Asset and BCA terms impacts the scope of the applicable requirements. The V5TAG recommends the following enhancements:
    - Clarify the intent of “programmable” in Cyber Asset.
    - Clarify and focus the definition of “BES Cyber Asset” including:

SAR Information

- Focusing the definition so that it does not subsume all other cyber asset types.
- Considering a lower bound to the term 'adverse' in "adverse impact".
- Clarifying the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that "N-1 contingency" is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope.

- Network and Externally Accessible Devices – V5TAG recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:
  - The 4.2.3.2 exemption phrase "between discrete Electronic Security Perimeters"
  - The meaning of the word 'associated' in the ERC definition.
  - The applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section.
  - The IRA definition placement of the phrase "using a routable protocol" in the definition and with respect to Dial-up Connectivity.
  - The Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."
- Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations – V5TAG is aware of multiple interpretations of the language "used to perform the functional obligation of" in CIP-002-5.1 Attachment 1, section 2.12 and recommends clarification of:
  - The applicability of requirements on a TO Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.
  - The definition of Control Center.
  - The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.
- Virtualization – The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider CIP-005 and the definitions of Cyber Asset and Electronic Access Point regarding permitted architecture and the security risks of network, server and storage virtualization technologies.

The SDT shall also address the Order No. 822 directives by developing modifications to requirements in CIP standards and the definition of LERC. The Commission directed the following:

- *Per paragraph 32, "...we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by*

SAR Information
transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards." • *Per paragraph 53, "…the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."* • *Per paragraph 73, "…the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule…."*

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.

Reliability Functions		
☒	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☒	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☐	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and Reactive Power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☐	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and Reactive Power supply and demand.

Reliability and Market Interface Principles	
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	YES
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	YES
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	YES
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	YES

Related Standards	
Standard No.	Explanation

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
FRCC	
MRO	
NPCC	
RF	
SERC	
SPP RE	
Texas RE	
WECC	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards Standards Authorization Request (SAR)

Do not use this form for submitting comments. Use the electronic form to submit comments on the **Project 2016-02 Modifications to CIP Standards SAR**. The electronic comment form must be submitted by **8 p.m. Eastern, Thursday, June 30, 2016**.

Additional information about this project is available on the Project 2016-02 Modifications to CIP Standards page. If you have questions, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

Background Information

On January 21, 2016, the Commission issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards,* approving seven CIP Reliability Standards and new or modified definitions. On March 9, 2016, the NERC Standards Committee accepted the Standards Authorization Request (SAR) and authorized the posting of the Modifications to CIP Standards SAR. It was posted for a 30-day informal comment period March 23 – April 21, 2016. Based on the comments received, the Standard Drafting Team (SDT) made minor revisions to the SAR which will be posted for an additional 30-day informal comment period.

It was noted in the comments received on the SAR that the Virtualization issue involved more than just CIP-005 standards and the defined terms Cyber Asset and Electronic Access Point. To correct this, the SDT revised the sentence to: "Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider ~~CIP-005 and the definitions of Cyber Asset and Electronic Access Point~~ the CIP V5 standards and the associated definitions regarding permitted architecture and the security risks of ~~network, server and storage~~ virtualization technologies."

Other commenters suggested that the SDT include provisions to address CIP Exceptional Circumstances. A sentence was added to the SAR to include this topic: "In addition, the SDT will review and address the CIP V5 requirements for CIP Exceptional Circumstances exceptions."

A sentence was also added to the SAR allowing the SDT to make errata changes to the standards as necessary and to correct grammatical, punctuation and/or formatting errors in the V5 Standards: "Finally, the SDT will review the Guidelines and Technical Basis sections of the CIP V5 standards and adjust where appropriate as well as correct any grammatical, punctuation, and/or formatting errors, and make other errata changes to the CIP V5 standards, as necessary."

In the previous version of the SAR, the Transmission Service Provide (TSP) Reliability Function was checked as an applicable function. The TSP is not applicable under the CIP standards and this function was corrected by unchecking the TSP Reliability Function in this version of the SAR. Similarly, the Distribution

Provider (DP) Reliability Function was left unchecked in the original SAR. The CIP Standards apply to the DP, so this was corrected by checking the DP Reliability Function in this version of the SAR.

Questions

1. The CIP SDT revised the SAR based on the comments received in the previous posting as noted above. Do you agree with these revisions to the SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

   Yes:

   No:

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP V5 Issues for Standard Drafting Team Consideration

September 15, 2015

From experience in the V5 Transition Study and the on-going implementation efforts, the CIP Version 5 Transition Advisory Group (V5TAG) identified specific issues with the CIP Version 5 standard language that caused difficulty in implementation of the requirements. In many cases, the V5TAG members found that select language within the CIP Version 5 standards may be understood in multiple ways. These interpretations appear to go beyond the intended flexibility of the standard language that is necessary to accommodate the diverse nature of facts and circumstances across the electric sector. At this time, the V5TAG proposes the following issues to be addressed by the CIP V5 Revisions drafting team (SDT) or other appropriate team for standards development:

- **Cyber Asset and BES Cyber Asset definitions**

  The foundational definition for the CIP Version 5 standards is 'Cyber Assets.' When Cyber Assets meet a threshold of Bulk Electric System (BES) impact they become 'BES Cyber Assets (BCA)' which are grouped, by a Responsible Entity, into 'BES Cyber Systems (BCS).' Viewing BCAs too broadly can lead to many thousands of devices in the typical utility becoming an administrative burden for which few if any cyber security controls can actually be applied or where there is limited associated cyber security risk. Vast amounts of effort would be expended for these types of cyber assets to track and document their lack of capability for even the most basic cyber security controls. Viewing BCAs too narrowly could lead to missing consideration of devices that have a sufficient level of cyber capability and risk impact.

  The SDT should consider the definition of Cyber Asset and clarify the intent of "programmable" by considering such factors as if a device is merely configurable, its executable code is not field upgradable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc.

  The SDT should consider clarifying and focusing the definition of "BES Cyber Asset" including:

  a. Focusing the definition so that it does not subsume all other cyber asset types. Protected Cyber Assets (PCA), by nature of being on the same network, can have some form of adverse impact if misused. Electronic Access Control or Monitoring Systems (EACMS) if misused or unavailable can have some form of adverse impact. This can result in a "hall of

mirrors" effect where everything in or that creates an Electronic Security Perimeter (ESP) also meets the BCA definition.

b. Considering if there is a lower bound to the term 'adverse' in "adverse impact". For example, is the focus of a typical generating unit the servers and operator human machine interfaces (HMI) and controller cabinets and Programmable Logic Controllers (PLCs) or is it the thousands of individual sensors and transmitters throughout the plant?

c. Clarify the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that "N-1 contingency" is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope.

- **Network and Externally Accessible Devices (ERC, ESP, IRA)**

  The SDT should consider the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:

  a. Clarify the 4.2.3.2 exemption phrase "between discrete Electronic Security Perimeters." When there is not an ESP at the location, consider clarity that the communication equipment considered out of scope is the same communication equipment that would be considered out of scope if it were between two ESPs.

  b. The word 'associated' in the ERC definition is unclear in that it alludes to some form of relationship but does not define the relationship between the items. Striking 'associated' and defining the intended relationship would provide much needed clarity.

  c. Review of the applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section. As well, consider the interplay between IRA and ERC.

  d. Clarify the IRA definition to address the placement of the phrase "using a routable protocol" in the definition and clarity with respect to Dial-up Connectivity.

  e. Address the Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."

- **Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations**

  CIP-002-5.1 Attachment 1 – Impact Reliability Criteria, sections 1.1, 1.2, 1.3, 1.4, 2.11, 2.12, and 2.13 employ the language "used to perform the functional obligation of", and then lists the functional registration. It was intended that this caveat would capture entities that perform obligations of a specific registered function, whether they are registered for that function or not. However, this language has caused confusion, especially in section 2.12 concerning TOP Control Centers. The term "functional obligation" may be interpreted to have different meaning in a variety of situations.

One interpretation is for the defined term Control Center to be strictly associated with the Balancing Authority (BA), Generator Operator (GOP), Reliability Coordinator (RC), and Transmission Operator (TOP) functional registrations, and that control rooms or dispatch centers owned and operated by Transmission Owners (TOs) with control of limited BES facilities would be excluded. A second interpretation may expand or contract the applicability of the Control Center designation, based on criteria that may not take into consideration overall risk to reliable operations of the BES.

Early analysis found the potential for TOs (not Registered as TOPs) that only operate limited breakers to be pulled in as medium impact Control Centers, even if the few Facilities they control are low impact. (For example, an entity with one 161kV breaker in one substation and a second 161kV breaker in a different substation, both breakers associated with low impact Facilities.) As currently written, low impact Control Centers are to be identified per criteria 3.1 and could be commensurate with risk for these scenarios.

Areas for the SDT to address are:

a. CIP-002-5.1, Attachment 1 Control Center criteria for additional clarity and for possible revisions related to TOP or TO Control Centers performing the functional obligations of a TOP, in particular for small or lower-risk entities. A potential revision could be a size for criteria 2.12, Control Centers performing the functional obligations of a TOP.
b. Clarify the applicability of requirements on a TO Control Center that perform the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES. Review the corresponding Guidelines and Technical Basis of CIP-002-5.1, specifically: the "CIP-002-5" section paragraph starting with "Responsibility for the reliable operation of the BES is spread across all Entity Registrations"; the table following that paragraph; the "High Impact Rating (H)" section; and the criterion bullets for Control Centers under the "Medium Impact Rating (M)" section.
c. The definition of Control Center (if pursued, recognize possible impacts on operations and planning standards and/or glossary terms that include 'Control Center', for example, the revised Glossary term for "System Operator" to be effective July 1, 2016).
d. The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.

- **<u>Virtualization</u>**

  The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration.

The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies.

The transition to CIP Version 5 continues as the compliance deadline of April 1, 2016 approaches. The V5TAG continues to discuss challenging issues being undertaken during the on-going implementation. The group may find additional issues to transfer to the SDT for consideration.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards Standards Authorization Request

Informal Comment Period Open through April 21, 2016

Now Available

A 30-day informal comment period for the **Project 2016-02** Standard Authorization Request (SAR), is open through **8 p.m. Eastern, Thursday, April 21, 2016**.

Commenting

Use the electronic form to submit comments on the SAR. If you experience any difficulties in using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 8 p.m. Eastern).

Next Steps

The drafting team will consider all responses received during the comment period and determine the next steps of the project

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comments
Received Report

Project Name:	2016-02 Modifications to CIP Standards SAR
Comment Period Start Date:	3/23/2016
Comment Period End Date:	4/21/2016
Associated Ballots:	

There were 33 sets of responses, including comments from approximately 33 different people from approximately 32 companies representing 9 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

3. Are there any other concerns with this SAR that haven't been covered in the previous questions?

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Florida Municipal Power Agency	Chris Gowder	3,4,5,6	FRCC	FMPA	Tim Beyrle	Florida Municipal Power Agency	4	FRCC
					Jim Howard	Florida Municipal Power Agency	5	FRCC
					Lynne Mila	Florida Municipal Power Agency	4	FRCC
					Javier Cisneros	Florida Municipal Power Agency	3	FRCC
					Randy Hahn	Florida Municipal Power Agency	3	FRCC
					Don Cuevas	Florida Municipal Power Agency	1	FRCC
					Stan Rzad	Florida Municipal Power Agency	4	FRCC
					Matt Culverhouse	Florida Municipal Power Agency	3	FRCC
					Tom Reedy	Florida Municipal Power Agency	6	FRCC
					Steve Lancaster	Florida Municipal Power Agency	3	FRCC
					Mike Blough	Florida Municipal Power Agency	5	FRCC
					Mark Brown	Florida Municipal Power Agency	4	FRCC

					Chris Adkins	Florida Municipal Power Agency	3	FRCC
					Ginny Beigel	Florida Municipal Power Agency	9	FRCC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Southwest Power Pool, Inc. (RTO)	Jason Smith	2	MRO,SERC,SPP RE,WECC	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Jason Smith	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Ellen Watkins	Southwest Power Pool, Inc. (RTO)	1	SPP RE
					Terri Pyle	Southwest Power Pool, Inc. (RTO)	1,3,5,6	SPP RE
					Mike Buyce	Southwest Power Pool, Inc. (RTO)	1,4	SPP RE
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Robert A. Schaffeld	Southern Company - Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Southern Company - Southern Company Services, Inc.	3	SERC
					William D. Shultz	Southern Company - Southern Company Services, Inc.	5	SERC

					John J. Ciza	Southern Company - Southern Company Services, Inc.	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6	NPCC	RSC No Dominion	Paul Malozewski	Northeast Power Coordinating Council	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Brian Shanahan	Northeast Power Coordinating Council	1	NPCC
					Rob Vance	Northeast Power Coordinating Council	1	NPCC
					Mark J. Kenny	Northeast Power Coordinating Council	1	NPCC
					Gregory A. Campoli	Northeast Power Coordinating Council	2	NPCC
					Randy MacDonald	Northeast Power Coordinating Council	2	NPCC
					Wayne Sipperly	Northeast Power Coordinating Council	4	NPCC
					David Ramkalawan	Northeast Power Coordinating Council	4	NPCC

Glen Smith	Northeast Power Coordinating Council	4	NPCC
Brian O'Boyle	Northeast Power Coordinating Council	5	NPCC
Brian Robinson	Northeast Power Coordinating Council	5	NPCC
Bruce Metruck	Northeast Power Coordinating Council	6	NPCC
Alan Adamson	Northeast Power Coordinating Council	7	NPCC
Michael Jones	Northeast Power Coordinating Council	3	NPCC
Michael Forte	Northeast Power Coordinating Council	1	NPCC
Kelly Silver	Northeast Power Coordinating Council	3	NPCC
Brian O'Boyle	Northeast Power Coordinating Council	5	NPCC
Edward Bedder	Northeast Power Coordinating Council	1	NPCC
David Burke	Northeast Power	3	NPCC

						Coordinating Council		
					Peter Yost	Northeast Power Coordinating Council	4	NPCC
					Helen Lainis	Northeast Power Coordinating Council	2	NPCC
					Michele Tondalo	Northeast Power Coordinating Council	1	NPCC
					Kathleen Goodman	Northeast Power Coordinating Council	2	NPCC
					Silvia Parada Mitchell	Northeast Power Coordinating Council	4	NPCC
					Sylvain Clermont	Northeast Power Coordinating Council	1	NPCC
					Si Truc Phan	Northeast Power Coordinating Council	2	NPCC
Colorado Springs Utilities	Shannon Fair	1,3,5,6		Colorado Springs Utilities	Kaleb Brimhall	Colorado Springs Utilities	5	WECC
					Charlie Morgan	Colorado Springs Utilities	3	WECC
					Shawna Speer	Colorado Springs Utilities	1	WECC

					Shannon Fair	Colorado Springs Utilities	6	WECC

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	

The SPP RE respectfully submits the following eight comments to the Project 2016-02 Standards Authorization Request: (1) With respect to clarifying or revising the definition of Cyber Asset, consider including misuse of the Programmable Electronic Device through misconfiguration or reconfiguration of the device in the instance that its behavior is affected and its altered behavior impacts the associated Facility. Consider the risk of misuse (i.e., how would someone misconfigure or reconfigure the device to cause undesired behavior) as appropriate. (2) With respect to clarifying or revising the definition of External Routable Connectivity (ERC), consider the point in the communication path at which a conversion from routable to non-routable communication protocol occurs. Is ERC only established if the conversion occurs in the same asset as the BES Cyber Asset or can ERC be established if the conversion occurs at the remote end of the communication path (e.g., conversion at the Control Center for communication to a serially connected relay in a substation)? Consider whether ERC exists only if the conversion occurs outside of an established ESP (i.e., there is no ERC if the device performing the conversion is inside an ESP and protected per the CIP Standards). (3) With respect to CIP-002-5.1, Impact Rating Criteria 3.2 and 3.3, clarify that the Low Impact BES Cyber Systems are associated with Facilities located within the asset as opposed to being associated with the asset itself. The opening statement in Section 3 of the Impact Rating Criteria states "BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets…" The SPP RE has already been presented with an argument that flow meters in a substation are not BES Cyber Assets because they are associated with a Transmission line and not the Transmission station or substation cited in Impact Rating Criterion 3.2. (4) With respect to Tie Line and other Transmission line flow meters, these Cyber Assets appear to have been unintentionally excluded from consideration under CIP-002-5.1, Impact Rating Criterion 2.5. Impact Rating Criterion 2.5 excludes consideration of BES Cyber Assets associated with Transmission lines through its use of "operating between 200 kV and 499 kV at a single station or substation" language. In the instance where the tie line or other flow meter is associated with a Transmission Line operated between 200 and 499 KV in a substation that satisfies the qualifications of Impact Rating Criterion 2.5, the meter will be excluded and not be categorized as Medium Impacting. Additionally, some entities are proffering the argument that the flow meter is not a BES Cyber Asset because its loss or misuse will not affect the reliable operation of the Transmission Facilities in the substation where the meter resides, overlooking the impact the loss of meter information may have on Control Center operations including ACE calculation, security-constrained generation dispatch, AGC, and Situational Awareness. An additional Criterion, specific to Transmission line flow meters, may be required to address this issue. (5) With respect to Physical Security Perimeters and their associated Requirements, clarification is needed regarding the concept of zoned access within a defined PSP. Specifically, is it acceptable to define an overarching PSP and then establish areas of access control within the defined PSP where BES Cyber Systems are present and for which different access permissions are established? For example, can a building containing a Control Center and its associated data center be declared a single PSP while access controls are established that do not permit all personnel with authorized unescorted access into the building to have authorized unescorted access into one or more access control zones within the building (e.g., the data center). And, if the zoned access areas are deemed to be independent PSPs, would the application of CIP-006-6 R1 Part 1.3 require two access controls to enter the interior PSP containing High Impact BES Cyber Systems, or would the requirement for two access controls to enter the outer (building) PSP suffice such that a single access control is permitted for the interior PSPs? (6) In consideration of the results of the investigation of the Ukraine cyberattack, the SPP RE recommends that Cyber Assets outside of the ESP with a machine-to-machine connection to a Cyber Asset inside the ESP be subjected to the same controls as the Intermediate System. There is a gap in the Standards today whereby a communication protocol typically used for interactive access (e.g., FTP, SSH, web services) can also be used for system-to-system communication. While Interactive Remote Access requires the use of an Intermediate System, encryption, and multi-factor authentication to the

Intermediate System, system-to-system communication using the exact same protocols do not require such controls. The Electronic Access Point cannot tell the difference, thus a successful compromise of the Cyber Asset residing outside of the ESP affords the attacker trusted access into the ESP. (7) In consideration of the results of the investigation of the Ukraine cyberattack, the SPP RE recommends the Standards Drafting Team consider whether essential support systems (UPS, PBX/VOIP phone, fire suppression, emergency generation) should be afforded certain protective controls to mitigate the risk that a successful attack directed at the support systems would adversely impact the asset containing BES Cyber Systems. For example, one element of the Ukraine attack was directed at a network-connected Uninterruptible Power Supply, removing power from essential Cyber Assets. (8) The SPP RE understands that a number of Requests for Interpretation have been submitted against CIP Version 5. While NERC staff has stated publicly that the RFIs would be addressed by the Standards Drafting team, there is no mention of RFIs in the Standards Authorization Request. To the extent that there are RFIs not included in either the Order 822 or V5TAG items, the Standards Authorization Request should state that pending RFIs will be considered and addressed in any revisions to the CIP standards.

Likes 0	
Dislikes 0	

Response

Steven Parker - EnergySec - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

We recommend that the term, Adverse Impact, contained within the BES Cyber Asset definition be itself added as a defined Glossary term. Any attempt to clarify this phrase by adding language within the BES Cyber Asset definition is likely to complicate, rather than simplify, understanding of the term.

The current outstanding Requests For Interpretation should be added as issues to be addressed by the Standards Drafting Team under this SAR. Per the Standards Process Manual, Section 7, Interpretations “shall stand until such time as the Interpretation can be incorporated into a future revision of the Reliability Standard.” Although this statement does not directly apply to the currently open, and unresolved, Requests for Interpretation, we believe the most logical approach would be to address the identified issues via this SAR rather than a separate interpretation development effort.

We recommend that the scope of the SAR be expanded to address the increasing use of 3rd party (i.e. cloud) services. Numerous utilities are leveraging new capabilities available from 3rd party providers in ways that enhance the overall security of the grid. Examples include cloud-based vulnerability scanners, offsite log monitoring services, cloud-based malware analysis and threat detection, cloud-based network monitoring, and colocation facilities. Unfortunately, the current standards are unduly prohibitive towards these services and as a result may be lowering the overall security of the grid by discouraging the use of effective, cutting edge tools, techniques, and services. For example, CIP-006 requires EACMS devices to be within a Physical Security Perimeter. It is not clear how, or if, this requirement can be met for cloud services. The SDT should review existing language and add, modify, or remove language as needed to accommodate any such services that can be prudently deployed to enhance overall grid security.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	

Comment
Xcel Energy has some concern that the SAR's inclusion of communication network components between control centers could extend to cabling between Control Centers. The inclusion of cabling between Control Centers would be in direct contrast to guidance in the CIP standards and the authority granted in section 215(d)(5) of the FPA by asking entities to be held accountable for equipment they do not own. Communication networks between discrete Electronic Security Perimeters (ESPs) have been excluded from the CIP standards. Additionally, it is unclear how physical protection of cabling would afford any additional protection to networks already in compliance with the suite of CIP standards. Furthermore, the documentation of any physical protection would be administratively burdensome without adding any additional protection. If any requirement is to be added regarding cabling between Control Centers, we would encourage the drafting team to add it as logical controls such as encryption or other such measures under CIP-005 and/or CIP-007. To require physical protection of equipment not owned by Registered Entities seems in direct contrast to previous guidance, outside of the authority documented in section 215(d)(5) of the FPA and add administrate burden with little value.

Likes 0	
Dislikes 0	

Response

Ginny Beigel - City of Vero Beach - 9	
Answer	No
Document Name	

Comment
See response to Question 3.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
SMUD respectfully suggests an addition to the objective for this SAR be modified to include addressing single points of failure in communication networks and network equipment that meet the definition of the BCA where this equipment is outside of the ESP but contained within the Facility.	
Likes 0	
Dislikes 0	
Response	

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	

Seminole concurs with all items currently listed in the draft Standards Authorization Request. Seminole recommends that additional items should be included in the SAR

The industry has received guidance from NERC's Compliance Monitoring and Enforcement group in the form of Frequently Asked Questions and Lessons Learned. These guidance items need to become formal Guidelines, with appropriate Technical Basis, and placed within the Standards and approved by the NERC membership

Issues related to Shared Facilities that are not adequately addressed in the standards. Specifically, when multiple entities have BES Cyber Assets residing at a shared location, there is no clear delineation of responsibility. Without defined responsibilities in the Standard, there is also no documented process to determine who has responsibility and to document those responsibilities. CFRs, JROs, MOUs, and other contractual agreements have been discussed as possible solutions to this issue. However, at a minimum, clear formal Guidelines should be added to CIP-002-5.1. Additional guidance should be added where appropriate.

Based on experience of both the V5TAG and of entities preparing for the standards, it is clear that significant updates are needed to the Guidelines and Technical Basis for all CIP Reliability Standards.

Based on these comments, Seminole recommends adding language to address the following items:

1. **Guidelines and Technical Basis** – As core information used by Entities to ensure a consistent understanding of requirements and based on Lessons Learned by Entities, Reliability Standards CIP-002 through CIP-011 are authorized for modification by the Standards Development Team and submitted for ballot to the NERC Ballot Body. These clarifications should minimally consider
    i. Lessons Learned and FAQs published by NERC and Regional Compliance
    ii. Items that may be determined unsupported by the standard and definitions (i.e. BES Reliability Operating Services); and
    iii. Industry practices that have evolved from industry's compliance efforts.
2. **Paragraph 51 option** - Option to consider removal of Requirement Parts in specific cases considering the same guidelines as those used in the Paragraph 51 project.
3. **Definitions of Low Impact External Routable Connectivity AND External Routable Connectivity** - Consider modifying the definitions of External Routable Connectivity and LERC to ensure consistent language and communication of both ERC and LERC definitions
4. **Definitions of Cyber Asset, BES Cyber Asset (BCA), and BES Cyber System (BCS)** – The SAR should also authorize changes to clarify the definition of BES Cyber System, specifically whether BES Cyber Systems include any Cyber Asset type other than a BCA (such as PCA, EACMS, PACS)
5. **Measures and Audit Expectations** - Using information provided by the NERC Compliance Monitoring group as one source of information, the measures section of all requirements and requirements parts should be reviewed and updated as necessary to ensure that an entity who provides the evidence listed in the measure is able to fully demonstrate compliance under normal circumstances.
6. **Exceptional Circumstances** - Recommend formalizing guidance for Exceptional Circumstances in a single location.

Likes 0	
Dislikes 0	

Response

Andrew Pusztai - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC is a member of EEI and supports the comments submitted by the EEI CIP Standards Subgroup related to the draft SAR.

Likes 0	

Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The Edison Electric Institute (EEI) submitted comments relating to this SAR. Their comments address scope and objectives of the SAR for consideration by the Standards Drafting Team. Kansas City Power & Light Company endorses and incorporates by reference the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6 - NPCC, Group Name RSC No Dominion	
Answer	No
Document Name	
Comment	
Request that the scope of virtualization be expanded beyond only CIP-005. Want to remind the SDT that communications between Control Centers usually involves third parties that tend to be outside of FERC’s jurisdiction.	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	

Comment
The phrase “control centers” in the “Industry Need” section which lists the FERC directives has not been capitalized. FERC Order 822 uses “bulk electric system Control Centers” when speaking about this directive. Tri-State believes the SAR should use that same language used by FERC in order to accurately represent what is expected to be in scope of this project. There is also an error in the “Reliability Functions” section. “Transmission Service Provider” is checked off instead of “Distribution Provider”. The new versions of the CIP standards do not include Transmission Service Providers, but do include the Distribution Providers.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	

Comment
Virtualization: Manitoba Hydro does not agree with NERC prescribing specific system architecture, technologies or designs. The SDT should continue to focus on identifying requirements to meet specific security objectives for the virtualization. Protections for communication network components between control centers: Please clarify the scope of Control Centers. Does it refer to the communication links between all Control Centres cross entities such as the link between RC Control Center and TOP Control Centre or only the Control Centers within the resposbile entity.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	

Comment

FMPA is concerned that the Project 2016-02 SAR is too narrowly focused. There are a number of issues with the current CIP Standards, mostly concentrated in CIP-002-5.1. The SAR should be written to allow the drafting team to consider how the suite of CIP standards work together. CIP-002-5.1 is the foundation of the remainder of the CIP requirements. Narrowly scoping this SAR just prolongs dealing with these problems, and ties the drafting team's hands should they identify other concerns. Also, ignoring these issues now will cause more revisions, which in turn will add to the pervasive confusion and uncertainty already surrounding the CIP standards. The industry needs clarity and resolution to these matters in order to be assured their efforts to comply are effective and that companies understand their investments are going to the right places.

The following additional items should be considered by the SDT:

1) Section 4.2.2 states "All BES Facilities" as being subject to the standards for all Responsible Entities except for DP's. This effectively negates the rest of the requirements, as anything that qualifies as a "Cyber Asset" could not possibly be a "Facility" as well. The language is missing the "Cyber Assets" component. Suggested language would be "Cyber Assets at all BES Facilities".

2) Ownership isn't properly accounted for in the requirements. Shared facilities (generally speaking substations) often involve multiple entities that own equipment, who may or may not be Responsible Entities as described in CIP-002-5.1. There should be specific language requiring the owner of the equipment to communicate with the owner of the Facility.

3) Clarify what is meant by "associated with" in the context of the Impact Rating Criteria in CIP-002-5.1 – Attachment 1. Clear up the inconsistencies in the requirements between the use of "associated with" (criterion 2 & 3 in Attachment 1) in some areas and "used by and located at" (criterion 1 in Attachment 1) in other parts. Have a process developed for ensuring entities notify if there are devices owned by a different entity that are "associated with" their BESCS (for example, a meter that one entity needs for the reliable operation of their Control Center that isn't owned by them).

4) Leasing equipment is a loophole in the requirements based on the language in section 4.2. This should be fixed so an entity isn't able to lease equipment and avoid meeting CIP requirements.

5) The scope of equipment applicable to CIP due to applicability to other NERC standards (such as CIP-002-5.1 Section 4.2.1.3) should be clarified further. For example, a "Protection System" can be made up of multiple devices owned by multiple entities. If an entity owns a component of a Protection System that isn't a Cyber Asset, they shouldn't have to meet CIP requirements.

6) Voice over Internet Protocol (VoIP), much like virtualized servers and environments, is not discussed in the CIP requirements. VoIP telephony devices should be excluded from the requirements unless they are networked with other BESCS, in which case they could become protected CA's.

7) There is no mention of "data at rest" in this SAR, although it was clearly part of Order 822 (paragraph 56 – "NERC's response to the directives in this Final Rule should identify the scope of sensitive bulk electric system data that must be protected and specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted **or at rest**").

8) CIP-002-5.1 should be re-written to make sure all assets are properly identified. For example, under R1 of CIP-002-5.1, a Responsible Entity is only required to find Cyber Assets at each of the six locations listed under R1. However, in Attachment 1 for medium and low impact, the language of "associated with" is introduced, indicating that there could be assets/locations containing Cyber Assets that are not part of the list of six asset types listed under R1. The approach taken by R1 is not the one being recommended by NERC or the Regional Entities. The standard should be revised to clarify the relationship between the six asset types/locations in R1 and the "used by and located at"/ "associated with" language in Attachment 1.

Likes 0	
Dislikes 0	
Response	

Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	No
Document Name	
Comment	

The SAR should be modified to include the following language and scope:Update obsolete references to NERC defined terms or standards through modifications to the CIP standards. References which are obsolete or require clarification include, but are not limited to:

- To improve consistency within Registered Entity compliance programs, phrasing in CIP-002-5.1 Requirement 1 and Attachment 1 referencing undefined or unclear terms or phrases such as “Transmission stations and substations”, “generation interconnection Facilities”, “Systems and facilities critical to system restoration”, “Generation resources”, “BES reactive resource or group of resources” should be removed by the SDT and instead reference the FERC approved definition of Bulk Electric System (BES) which now included clear and defined qualifications for inclusion and exclusion of these assets as well as an appeals process to address exceptions. An example would be changing the following language:
- R1.ii. Stations and Substations containing BES Facilities
- R1.iii BES Generation Facilities
- RAS: Phrasing in CIP-002-5.1 Applicability, Requirement 1, and Attachment 1 referencing variations of Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements should be clarified and simplified by the SDT to reference the new Remedial Action Scheme (RAS) definition which FERC approved 11/19/2015.
- The current PSP definition should be clarified by the SDT to address that it should not apply to assets in CIP-006-6 Part 1.1 simply because they may be secured in a location which meets the PSP definition: “The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.”
- Interactive Remote Access definition: The SDT should clarify the phrase “system-to-system process communications” to address scripts or batch operations performed on-demand or on a periodic basis as not meeting the definition.
- The phrase “Collector Bus” as it appears in Attachment 1, Criteria 2.4 and 2.5 should be defined by the SDT. The guidance document references a report (*Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface*) which predated the adoption of the NERC BES definition and has not been picked up for development since. The BES definition provides additional clarification of the applicability to multiple generation scenarios in I2, I4, E1, E2, E3, and E4. Notably, CIP-014-1 does provide a diagram of the collector bus, but does not include an associated definition.
- Attachment 1, Criterion 2.4: Clarify if the Transmission Facilities operated at 500kV or higher are “at a single station or substation” to make the language and application consistent with Criterion 2.5 to correctly scope BES Cyber Assets.
- Clarify CIP-002-5.1 R1.vi for Registered Entities registered for additional functions other than Distribution Providers. Revising the language of CIP-002-5.1 R1.vi. to state “*For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above at assets which have not already been considered under Ri-Rv*” would be a possible solution.

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities agrees with the scope of the SAR.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
The Bureau of Reclamation believes that the proposed Standards Authorization Request addresses FERC directives in Order No. 822. Reclamation also supports NERC efforts to address the issues identified by the CIP Version 5 Transition Advisory group.	
Likes 0	
Dislikes 0	

Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	

Idaho Power agrees with the items that are currently scoped into the SAR, but also believe it does not go far enough. There are numerous areas within the v5/v6 standards where clarifications need to be made. Idaho Power doesn't think that a full re-write of all of the CIP standards is prudent as it will create continued churn in the industry. Idaho Power believes there should be continual slow improvement in the standards and not large swings that create guidance gaps from the regulators and understanding gaps from the industry.

The proposed scope does not include a change to the applicability columns to tier ratings (i.e., medium with and without ERC). These need to be more explicitly split out as they create odd breakdowns in the standards that seem to be creating inconsistencies in the standards. For example, under CIP-010-2 R4 Attachment 1, R1.2 requires authorizations for all Transient Devices and R3.1 for removable media for Medium Impact BCS. However, Medium Impact BCS without external routable connectivity (ERC) do not require an authorization records under CIP-004, specifically R4.1. This means the critical devices/systems themselves have no authorization requirements, but the transient devices and removable media associated with them do. A second example is information protection for Medium Impact BCS without ERC. CIP-011-2 requires information protection policies/procedures be applied equally to all Medium Impact BCS, which includes protecting it in storage, transit, and use. However, once again, there are no requirements to authorize an individual to gain access to "designated storage locations" under CIP-004-6 Part 4.1.3. This means the information needs to be protected, but only those Medium BCS with ERC have to have individuals get authorized for access to the information. This seems consistent with not authorizing individuals to get access to Medium Impact BCS without ERC but not with applying information protection policies to one tier of Medium Impact BCS.

The SDT should consider four risk tiers rather than three if they are going to treat ERC and non-ERC separately in the standards. These are simply two examples of inconsistencies that have been created by trying to treat them within the same "medium" risk tier. There could still be similar requirements that would be applied to a Medium Impact BCS with ERC and a Medium Impact BCS without ERC, but inconsistencies would be more easily identified by breaking out the Medium BCS tier and the Medium without ERC.

The proposed scope does not include changes to CIP-002-5.1. CIP-002 has several inconsistencies and logic issues and no clearly delineated process allowing no clear way to comply with the standard other than simply deciding on a direction and hoping the regional entity is okay with your approach. The wording and processes required by CIP-002 need to be refined and clarified to make the expectations more clearly known. For example, the Guidelines and Technical Basis state, "The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP [illegible] reference to use of the BROS is stated as an option that may be useful in identifying BCAs/BCSs. Nowhere in CIP-002 the definition of BCA or BCS does it speak directly to the BROS. The only loose tie-in is that the definition of BCS talks about reliability tasks, which FERC, in Order 791, clarified they believed it alluded to the NERC Functional Model, which relates to the high-level responsibilities of registered entities. However, it seems regions are beginning to take a stance that BROS is the hard-line approach as the only acceptable way to approach identification of CIP assets and BCAs/BCSs. Additionally, the wording of the CIP-002 standard does not ever specifically state that an entity needs to identify Protected Cyber Assets (PCAs), Electronic Access Control or Monitoring System (EACMS) or Physical Access Control Systems (PACS), yet the standards expect that entities will know what those devices are in order to apply specific requirements to them. Entities should not have to read between the lines when trying to comply with mandated compliance standards. Doing so creates confusion, inconsistencies, and distrust between the regulators and the industry who should be working together to meet common objectives.

Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT recommends that *Project 2016-02 – Modification to CIP standards* be limited to 1.) clarifying existing language,2.) addressing the V5 TAG issue list, and 3.) incorporating the FERC-directed changes discussed in FERC Order No. 822. Introducing new concepts through substantive language changes in this iteration would be premature. In order to allow CIP Version 5 and 6 concepts to be fully implemented, any proposed substantive changes should be reserved for future CIP standards projects.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Although Austin Energy (AE) agrees with the SAR's objectives, we urge the SDT to proceed with caution. Registered Entities are just now reaching compliance with the Version 5/6 Standards. Unless a device truly creates risk to the BES, we should not include it in the CIP Standards' scope.	
Likes 0	
Dislikes 0	
Response	
Jeri Freimuth - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes

Document Name	
Comment	

Arizona Public Service (AZPS) appreciates the opportunity to comment on the proposed SAR. Although AZPS generally supports the scope as described in the SAR, we believe that there are additional clarifications that should be considered beyond those detailed in the FERC Order 822 and the CIP Version 5 Transition Advisory Group (V5TAG) considerations.

AZPS believes the industry would benefit from clarification of the definition of the following terms:

- Transmission Facility – Transmission Facility is not a defined term. Although Facility is a defined term, AZPS does not believe that the Facility definition aligns with the standard's intent. AZPS suggests that a definition be provided by the Standard Drafting Team (SDT).

- Programmable - The SDT should consider defining programmable to clarify that a device would not be included simply because it was configurable, e.g., has functionality that can be changed locally.

AZPS would also like to suggest that the SDT clarify the intent of the grouping BCAs into BCS by leveraging the logically based perimeter security controls at the Electronic Security Perimeter (ESP) as well as local, device specific security controls per each BES Cyber Asset's (BCA) capability.

AZPS would also like to add some additional comments to the discussion in the V5TAG CIP V5 Issues for Standard Drafting Team Consideration document.

- AZPS recommends that the SDT consider not defining "adverse impact" or defining a lower bound thereof within the definition of BES Cyber Asset, but to revise the body of CIP standards and/or applicable defined terms to utilize already defined terms such as "Adverse Reliability Impact." Such would facilitate consistency as well as clarity regarding the N-1 contingency issue and other issues regarding that term identified by the V5TAG.

- AZPS believes that when BES Cyber Assets (BCA), such as relays, RTUs, and others, are connected via serial links to IP converters and/or IP-enabled security gateways, it would be appropriate to consider those elements downstream of the security gateways as BCA that do not have External Routable Connectivity (ERC). This is appropriate because the IP- converters and/or IP-enable security gateways require authentication and provide a protocol break. AZPS believes accurate and timely guidance related to serially connected devices supports the overall goal of providing appropriate and effective cyber security controls; thus, improving reliability.

- AZPS supports the CIP V5TAG analysis regarding virtualization. Virtualization is an effective tool for utilities and consideration should be given to ensuring that flexibility is maintained. An approach should consider the required outcome rather than the specifics of how that outcome is achieved.

Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF	

Answer	Yes
Document Name	
Comment	
Look to NIST 800-125 for virtualization security.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana McMahon - Salt River Project - 1,3,6,7 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Sistrunk - Small End-Use Electricity Customer - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Smith - Southwest Power Pool, Inc. (RTO) - 2 - MRO,SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.	
Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jason Smith - Southwest Power Pool, Inc. (RTO) - 2 - MRO,SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6 - NPCC, Group Name RSC No Dominion	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeri Freimuth - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Chris Sistrunk - Small End-Use Electricity Customer - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Diana McMahon - Salt River Project - 1,3,6,7 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginny Beigel - City of Vero Beach - 9	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Parker - EnergySec - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

3. Are there any other concerns with this SAR that haven't been covered in the previous questions?	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
The SDT should prioritize the issues based on whether it is associated with a FERC directive or not. For issues that are not directed by FERC, there may need to be additional time to find a resolution associated with these issues. The only deadlines on this project are related to the FERC directives.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Parker - EnergySec - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	2016-02_CIP_SAR_Unofficial_Comment_Form_ERCOT draft.docx
Comment	
Likes 0	
Dislikes 0	
Response	

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Smith - Southwest Power Pool, Inc. (RTO) - 2 - MRO,SPP RE, Group Name SPP Standards Review Group	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

Burns & McDonnell appreciates the opportunity to comment on the Standard Authorization Request (SAR) titled “Modifications to CIP Standards” with the following input:

The V5TAG recommended the Standard Drafting Team (SDT) consider Virtualization as part of the SAR due to the increased use of this technology in industry control system environments. Burns & McDonnell is recommending the Virtualization section of the SAR be amended to indicate that the SDT not only consider virtualization technology usage by Responsibility Entities (Entity) which they own and operate, but usage of similar technology not owned or operated by an Entity. Increased interest in “cloud” based services such as Software as a Service (SaaS) and Platform as a Service (PaaS) have created questions on the application of the standards with no guidance on how they should be applied. Cloud usage of virtual technology is similar to Entity owned usage of the same technology, but Burns & McDonnell feels it is important that both usage conditions be considered and any differences in approach be indicated in any final SDT work product. Burns & McDonnell does not believe a separate section should be created for “cloud” usage, but the SAR section on Virtualization could be updated to cover virtualization technology owned by or usage of services by an Entity. One recommendation for the re-wording is:

The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments either owned and operated by a Responsible Entity, or from a service provider who owns and operates the environment under the service providers control, V5TAG asked that the SDT consider CIP-005 and the definitions of Cyber Asset and Electronic Access Point regarding permitted architecture and the security risks of network, server and storage virtualization technologies under these two type of conditions.

Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	

Comment
Currently there are no specific requirements or guidelines included within the NERC CIP Reliability Standards v.5/6 relating to utilization of the cloud. Based on discussions with the regional auditing body, it has been agreed upon that utilization of the cloud for storage of BES Cyber System Information may be sufficiently secured through field level packet encryption with the responsible entity only holding the private key. It would be in the interest of the California ISO for there to be a provision included within the NERC CIP Reliability Standards addressing cloud scenarios.

Likes 0	
Dislikes 0	

Response

Ginny Beigel - City of Vero Beach - 9	
Answer	Yes
Document Name	

Comment
We belong to the FMPA municipal organization and have arrived at a consensus with the help of one of its SMEs who is immersed in CIP Standards. Comments follow below: The SAR falls short of fixing a lot of the core issues related to CIP-002-5.1. The following additional items should be addressed by the SDT: 1) Section 4.2.2 states “All BES Facilities” as being subject to the standards for all Responsible Entities except for DPs. This effectively negates the rest of the requirements, as anything that qualifies as a “Cyber Asset” could not possibly be a “Facility” as well. The language is missing the “Cyber Assets” component. Suggested language would be “Cyber Assets at all BES Facilities.” 2) Ownership isn’t properly accounted for in the requirements. Shared facilities (generally speaking substations) often involve multiple entities that own equipment, who may or may not be Responsible Entities as described in CIP-002-5.1. There should be specific language requiring the owner of the equipment to communicate with the owner of the Facility. 3) Clarify what is meant by “associated with” in the context of the Impact Rating Criteria in CIP-002-5.1 – Attachment 1. Clear up the inconsistencies in the requirements between the use of “associated with” (criterion 2 & 3 in Attachment 1) in some areas and “used by and located at” (criterion 1 in Attachment 1) in other parts. Have a process developed for ensuring entities notify if there are devices owned by a different entity that are “associated with” their BESCS (for example, a meter that one entity needs for the reliable operation of their Control Center that isn’t owned by them).

4) Leasing equipment is a loophole in the requirements based on the language in section 4.2. This should be fixed so an entity isn't able to lease equipment and avoid meeting CIP requirements.

5) The scope of equipment applicable to CIP due to applicability to other NERC standards (such as CIP-002-5.1 Section 4.2.1.3) should be clarified further. For example, a "Protection System" can be made up of multiple devices owned by multiple entities. If an entity owns a component of a Protection System that isn't a Cyber Asset, they shouldn't have to meet CIP requirements.

6) Voice over Internet Protocol (VoIP), much like virtualized servers and environments, is not discussed in the CIP requirements. VoIP telephony devices should be excluded from the requirements unless they are networked with other BESCS, in which case they could become protected CA's.

7) There is no mention of "data at rest" in this SAR, although it was clearly part of Order 822 (paragraph 56 – "NERC's response to the directives in this Final Rule should identify the scope of sensitive bulk electric system data that must be protected and specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted **or at rest**").

8) CIP-002-5.1 should be re-written to make sure all assets are properly identified. For example, under R1 of CIP-002-5.1, a Responsible Entity is only required to find Cyber Assets at each of the six locations listed under R1. However, in Attachment 1 for medium and low impact, the language of "associated with" is introduced, indicating that there could be assets/locations containing Cyber Assets that are not part of the list of six asset types listed under R1. The approach taken by R1 is not the one being recommended by NERC or the Regional Entities. The standard should be revised to allow for the proper capture of all Cyber Assets either ONLY at the six asset locations, OR both at these locations as well as any other associated location.

Likes 0	
Dislikes 0	
Response	
Diana McMahon - Salt River Project - 1,3,6,7 - WECC	
Answer	Yes
Document Name	
Comment	

For network and externally accessible devices, SRP agrees with improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA). However, SRP has additional concerns.

Although much of CIP-005-5 is compatible to CIP V3 requirements, it does include a new requirement related to IRA for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with ERC. R2.1 states: *Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.*

Based on R2.1 and the defined terms, demonstrating compliance with this requirement fundamentally requires evidence of two items:

1. That an Intermediate System is utilized such that the Cyber Asset initiating IRA does not **"directly access"** an applicable Cyber Asset; and

2. That technology for facilitating IRA meets the definition of an Intermediate System.

Issues with #1 – Ambiguity of "Directly Access"

In SRP's experience the ERO and Regional Entities have used undefined terminology such as "protocol break", "OSI layer 7 application break", "session break" and others to describe what is intended by or compliant with the phrase "does not directly access". However, SRP believes these terms mean different things to different subject matter experts and auditors. FERC articulated as much in Order 822. Although this issue has focused on LERC/LEAP requirements for low impact assets, the same ambiguity exists in the requirements for high/medium impact facilities. Where standards are unclear or ambiguous, entities are typically afforded flexibility in their compliance approaches. However, SRP believes the ERO has taken a rather prescriptive view of these requirements where reasonable people could easily differ in their interpretation. These ambiguities in defined terms and requirements need to be addressed by the SDT.

Issues with #2 – Ambiguity on acceptable Intermediate Systems

As noted in the Glossary of Terms, an Intermediate System is an Electronic Access Control or Monitoring System (EACMS). That notwithstanding, the ERO and Regional Entities have articulated rather informally and only fairly recently a need to assess each Intermediate System against the definition of BES Cyber Asset. This creates the potential for the proverbial "hall of mirrors" result, in the sense that individuals can rationalize a circumstance where seemingly all Cyber Assets (PACS, EACMS, other) could, under some scenario qualify as a BES Cyber Asset. SRP believes this was clearly not the intent of the Standard Drafting Team, and SRP does not believe this concept was considered for Intermediate Systems evaluated during the CIP V5 pilot project.

Most specifically, an entity that was on the drafting team and participated in the implementation pilot project with no issues was "surprised" with the Regional Entity's assessment of compliance on this subject at time of audit. There is clearly a disconnect that needs to be addressed.

Architectures to support Interactive Remote Access to high, medium impact control centers, transmission stations and generation resources are very costly. Current ambiguity could cause extensive and rework for high and medium impact systems, and be even more impactful if similar architectures are applied to low impact assets.

The Standards Drafting Team (SDT) must clearly define the term "direct access" for high and medium facilities, ensuring "direct access" has same meaning for low impact facilities as ordered by FERC in its approval of the CIP V5 revisions. To the extent different controls are appropriate for high/medium vs. low impact systems, those distinctions must be clear in the language of the standard. SRP further recommends the SDT re-evaluate the definitions of Interactive Remote Access, Intermediate System, and BES Cyber Asset to ensure entities have a clear understanding of the security and compliance expectations associated with the standards.

Likes 0	
Dislikes 0	
Response	
Chris Sistrunk - Small End-Use Electricity Customer - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

I believe that the CIP standards do not properly address security monitoring of networks (routable and non-routable). In my experience in the security industry that breaches (like electric disturbances) are inevitable, even for control systems. It's a matter of when, not if. The Security Event Monitoring logging requirements in CIP 007-5 R4 is a start, but I don't believe this data (4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.) provides enough digital forensic evidence in the aftermath of an intrusion or even a cyber attack. Also, the retention period in 4.3 of a minimum of "90 consecutive calendar days" is not sufficient. According to the 2016 M-Trends Report from FireEye (https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf), the median time of network compromise to discovery of the attacker is 146 days. If a utility only kept 90 days of logs, then it's quite possible that they won't have the forensics data to determine if the attacker used stolen credentials or malicious code. Also, many utilities don't use authentication or encryption with their Control System Protocols such as DNP3, ICCP, and Modbus. If an attacker were to spoof, replay, or modify the SCADA traffic, this would not be detected by the current set of monitoring and logging requirements.

However, IT security best practice of network security montoring (NSM) does provide sufficient network forensics data. NSM is similar to the type of monitoring and visibility required by NERC PRC 002-2 Disturbance Monitoring and Reporting standard. I wrote a blog post (https://www.linkedin.com/pulse/comparing-nerc-disturbance-monitoring-reporting-network-sistrunk) about the similarities between PRC 002-2 and NSM...and how NERC CIP 007 R4 could be improved to provide a bit more forensics data. Collecting NSM type data such as Session Data (timestamp, source IP address, source port, destination IP, destination port at a minimum) does not require a lot of storage space and would provide a better level of visibility. Collecting a shorter time period of full network packet captures for High or Medium BES Cyber Systems (including non-routable dial-up access) also is not very complicated, as IT systems have been doing this a long time.

Since BES systems are becoming more connected, we cannot ignore network security monitoring in the future. I hope it doesn't take a serious cyber incident to convince the need for monitoring...much like the 1965 and 2003 blackouts convinced us to do disturbance monitoring. I know we haven't had a cyber attack that caused a power outage here in North America, but as an Electrical Engineer who has worked in the electric utility industry, now representing the ICS security industry, and also a customer, I want to help ensure that this doesn't happen.

Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy requests that the SDT consider revisiting the transfer of employees and the requirement to remove access for that employee in 1 calendar day which may be viewed as overly burdensome. While this may be outside the scope of this particular SAR, we feel that since the project is regarding revisions to CIP standards, that we would be remiss not to request further discussion around this topic.	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
ATC is a member of EEI and supports the comments submitted by the EEI CIP Standards Subgroup realted to the draft SAR. Please review for applicability to this question.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE noticed there is a statement on page 4 which says the compliance deadline is April 1, 2016. This has been moved back to July 1, 2016.	

Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

In addition to the issues addressed by the SAR, the Edison Electric Institute, on behalf of our members, recommends that the proposed project also consider the following ten issues:

Issue 1: CIP Exceptional Circumstances

A CIP Exceptional Circumstance is defined as:

"A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability."

We appreciate the understanding and recognition for the need to enable provisions for CIP Exceptional Circumstances. However, during implementation of CIP V5, it has become apparent that the CIP Exceptional Circumstances provision may need to be added to several requirements. Below are a few situation-based examples:

- *Risk of injury or death*: CIP-004-6 R2 and R4 allow for CIP Exceptional Circumstances to waive the need for Training and the Authorization based on need to be waived during such circumstances. We believe that CIP-004-6 R3 also should allow for CIP Exceptional Circumstances because the requirement to obtain a Personal Risk Assessment takes additional time that would hinder the ability of first responders to enter a Physical Security Perimeter in the event of the need for life saving measures. This would be consistent with CIP-004-3 "except in specified circumstances such as an emergency."
- *Impediment of large scale workforce availability*: CIP-007-6 R2 Security Patch Management requirements may be difficult to meet in the event that a major storm impacts a responsible entity, which requires all employees to report for storm duty for restoration efforts.
- *Natural disaster*: CIP-006-6 R1 Part 1.4 monitoring may not be possible if the physical access point to a PSP is under water or destroyed by a storm. Similarly, Part 1.3 causes compliance issues if for example, a fire renders a PACS controller panel inoperable and the PSP access points have failed secure. Emergency response may have to use a physical key, mechanical lock, or an axe to gain access. Without the IAC language or CIP Exceptional Circumstance provision, PSP access point monitoring is a zero defect issue.

We recommend that the SDT review all of the requirements of CIP V5 to determine whether: a CIP Exceptional Circumstances provision should be added, the definition of CIP Exceptional Circumstances should be edited, and/or additional explanatory language should be added to the Guidelines and Technical Basis for each standard regarding CIP Exceptional Circumstances.

Issue 2: BES Cyber Asset definition – "redundancy"

The application of the redundancy clause in the BES Cyber Asset (BCA) definition is unclear because the use of different and separate technologies and methods reduce reliability risk by providing alternative data sources. For example, VoIP systems, data center phone systems, radios, and other backup communication systems are alternatives, yet could be considered redundant by auditors and therefore it is unclear whether there are limits to the application of the BCA adverse impact to these systems. Without such limitations, the BCA definition may encourage registered entities to reduce their use of backup/alternative systems to reduce their compliance burdens and risk. While redundant assets may typically have identical security risks and vulnerabilities, requiring both/all to be similarly protected, alternative systems or assets are often substantially different and have drastically dissimilar risks and vulnerabilities, which reduces overall risk to the BES.

Issue 3: VoIP as a BES Cyber Asset

CIP-002-5.1 4.2.3.2 exempts "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters" from CIP-002-5.1; however, the Guidelines and Technical Basis for CIP-002-5.1 calls out operational directives (TOP, RC, BA) as an aspect of Inter-Entity Coordination and Communication function. As a result, some auditors are viewing VoIP as in scope for CIP-002-5.1 despite the exemption and fact that different and separate communication technologies are used for this function. If the exemption does not apply, then the BES Cyber Asset definition should also apply; however, EEI members are hearing that auditors do not agree and believe that VoIP used for operational directives are BES Cyber Assets even if the 15 minute impact does not apply due to the redundancy issue mentioned above.

We recommend that the SDT consider these issues and determine how best to address VoIP in the standard that is aligned with the risk to the bulk electric system.

Issue 4: LERC definition application to assets located external to the low impact asset

The last three asset classes in CIP-002-5.1 R1 are typically implemented across multiple instances of the first three classes (i.e., systems and facilities critical to system restoration, special protection systems, and distribution provider protection systems are typically implemented at control centers, substations, and generating resources).

The Low Impact External Routable Connectivity (LERC) definition appears to be based on single asset locations ("direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset ***outside the asset*** containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection.") The phrase "outside the asset" can cause confusion in determining whether LERC exists for these classes of assets that are implemented across multiple sites.

For example, when evaluating a cranking path as an asset to determine if it has LERC, what does "outside the asset" mean? This could also allow for routable protocol based communication within the multiple substation cranking path to not be considered LERC and left unprotected if the entire cranking path is considered a single "asset containing low impact BES Cyber Systems." It appears these last 3 asset classes are actually criteria that should affect the categorization of the single site asset class where they are implemented.

Issue 5: Custom software (scripts)

CIP-010-2 R1, Part 1.1, subpart 1.1.3 requires a baseline configuration for "any custom software installed." The Guidelines and Technical Basis for this requirement states that "custom software installed may include scripts developed for local entity functions." It is unclear whether all scripts must be considered custom software or whether only scripts that can have an impact on the bulk electric system within 15 minutes must be considered custom software under this requirement. A risk-based clarification should be added to this requirement to set boundaries as to what is considered custom software. For example, a script that alters the behavior or function of a BES Cyber Asset or System should be included; however, a script that simply gathers log data, and whose only impact to the BES Cyber Asset is the allocation of incidental CPU cycles, need not be included.

Issue 6: Applicability of the requirement part to Cyber Asset vs. Cyber System

Some requirements such as in the CIP-007-6 standard apply to Cyber Assets within a BES Cyber System (e.g., the R2 security patch management requirements), others apply at either the BES Cyber System level or Cyber Asset level (e.g., the R4 Part 4.1 logging requirements), and others don't specific if they apply at the system or asset level (e.g., R3 Part 3.1 method to deter, detect, or prevent malicious code). Although the applicable systems for each of these requirements is generally the same (i.e., high and medium impact BES Cyber Systems and their associated EACMS, PACS, and PCA), the difference in the requirements language applicability to Cyber Assets, BES Cyber System, or both makes what is necessary to comply with the requirements unclear.

For example, the requirements section for CIP-007-6 R3 Part 3.1 does not specify whether this requirement applies at the BES Cyber System level or Cyber Asset level, therefore it is unclear whether a responsible entity can protect a medium impact BES Cyber System through deploying an anti-virus solution at the BES Cyber System level or whether the entity must deploy the solution at each Cyber Asset to comply with the requirement part. Consistency among the requirements language would be helpful in clearing up this confusion.

Issue 7: Control Center definition

The NERC document titled "CIP V5 Issues for Standard Drafting Team Consideration" already raises issues with the Control Center definition related to Transmission Owner Control Centers; however, it does not address issues related to Generator Operators.

By definition, a Control Center is "one or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers … 4) a Generator Operator for generation Facilities at two or more locations."

Dispersed or distributed generation facilities (e.g., wind, solar, hydro) may not have the traditional control building with a horseshoe operator control desk ("facility hosting operating personnel that monitor and control"). Does the facility have to perform all "real-time … reliability tasks" or as few as one? Does a control room at a single wind farm, which controls a hundred turbines spread over many miles, meet the control center definition or does it become a control center only if it controls multiple wind farms? Also, if personnel maintains the Cyber Assets (e.g., patching or troubleshooting) is this considered "monitor and control" even though they are not personnel performing real-time reliability tasks. Does operating personnel mean those charged with the responsibility to monitor and control the BES or simply personnel who may be located at the generation Facility to maintain the equipment? Also, do each of the "generation Facilities at two or more locations" need to meet the Bulk Electric System definition to be within scope of the Control Center definition? CIP-002-5.1 Requirement R1, iii uses Generation resources, which could be interpreted to include all generation sources, even those that do not meet the Bulk Electric System definition.

As dispersed or distributed generation increases, clarity in language of the standard will become more important.

Issue 8: Security patches for operating Cyber Assets brought into scope under CIP V5

CIP-007-6 R2, Part 2.2 is clear concerning the ongoing evaluation of security patches as of July 1, 2016, but is unclear on what is required for the initial execution of the process ("evaluate security patches for applicability that have been released since the last evaluation") when there is no "last evaluation."

The standard does not require all Systems to be updated by July 1, 2016, but does require a baseline configuration, which includes a listing of all applied patches. The Guidelines and Technical Basis for CIP-010-2 states that "security patches applied would include all patches that have been applied on the cyber asset… CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches." This documentation requirement is particularly burdensome for an asset that has been in service for six years or longer as it requires entities to contact and work closely with their vendors to identify and get historical security patches. Also, documenting all historical patches, especially those that happened years ago will have little, if any impact on reliability.

Issue 9: Guidance for Secure Interactive Remote Access

In the Guidelines and Technical Basis for CIP-005-5, under Requirement R2 it states: “see Secure Remote Access Reference Document (see remote access alert).” Also, the Rationale for R2 states “Additional information is provided in Guidance for Secure Interactive Remote Access published by NERC in July 2011.” We believe these references are to the same document, which is properly titled under the Rationale and note that the 2011 NERC document was written in the context of V3 and not V5. Please evaluate the relevance of this guidance document to the most recent version (currently CIP-005-5). Also please clarify that IRA is intended to address access remotely from outside the organization (i.e., not to include accesses internally between protected networks).

Issue 10: Mistakes in Guidelines and Technical Basis

In implementing CIP V5, we’ve noticed a number of mistakes, which should be addressed, including:

- The rationale statements from the -5 standards were lost in several of the -6 versions of the standards. For example, the second sentence of the CIP-007-5 R2 rationale “The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.” was not carried forward to the -6 Guidelines and Technical Basis, even though there were no changes to the requirement between versions. We recommend reviewing the Rationales in the -6 standards and adding any that were deleted to the Guidelines and Technical Basis of the standard.
- For CIP-007-6 Part 2.2 the Guidelines and Technical Basis states: “Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.” However there are no CIP-007-6 R2 Parts have TFE provisions.
- For CIP-004-6 R4, under the Guidelines and Technical Basis, the Rationale for this requirement states: “to ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. “ ‘Authorization’ should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants ***and included in the delegations referenced in CIP-003-6***” CIP V3 required designating approvers; however this requirement was not included in CIP-003-6 and therefore the emphasized text should be removed***.***
- For CIP-004-6 R4, the Rationale also references “quarterly reviews in Part 4.5”; however there is no Part 4.5 in CIP-004-6 R4.

Likes 0	
Dislikes 0	

Response

Jeri Freimuth - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

NERC’s webpage for this SAR “Project 2016-02 Modifications to CIP Standards”, as of 4/11/2016, states the following:

“Also the scope of this work will incorporate existing and future RFIs relating to the CIP-002 through CIP-011 family of standards.”

AZPS does not believe any RFIs are addressed in the current SAR. We recommend updating the SAR to reference existing submitted RFIs as appropriate. Finally, AZPS recommends removal from the SAR of functional registrations that are no longer included in the Compliance Registry, e.g., Interchange Authority, Load-Serving Entity and Purchasing-Selling Entity.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6 - NPCC, Group Name RSC No Dominion	
Answer	Yes
Document Name	
Comment	
Request that the SAR explicitly reference the correct title of the V5 TAG document, which we believe is “CIP V5 Issues for Standard Drafting Team Consideration, “dated on September 15, 2015.	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Distribution Provider is not checked as an affected Reliability Function.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	
Document Name	4-15-16 DRAFT CIP V5 Implementation Issues.pdf
Comment	
Southern supports the comments of EEI. See attached.	
Likes 0	
Dislikes 0	
Response	

Comments received from Ginette Lacasse, Seattle City Light

Here are our Subject Matter Expert's (SME) comments. Non-italicized text is copied from SAR, with SME additions in RED. Additional SME comments are *in italics*.

Questions

1. **Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.**

Yes:
No: X

Comments:

In several sections the language of the SAR summarizes that of the foundation V5TAG document, but in doing so conflates or glosses over important concepts. Seattle City Light would like to see clarification to the SAR in the following two sections: (added text in red to clarify)

A) Cyber Asset and BES Cyber Asset (BCA) Definitions – as foundational definitions within the CIP V5 standards, the understanding of Cyber Asset and BCA terms impacts the scope of the applicable requirements. 'Right-sizing' the definitions of "Cyber Asset" and "BES Cyber Asset" balances between the administrative burden and negligible security benefit of an overly broad interpretation and the cyber security risk of too narrow an interpretation. The V5TAG recommends the following enhancements:

- Clarify the intent of “programmable” in Cyber Asset.
- Clarify and focus the definition of “BES Cyber Asset” including:
- Focusing the definition so that it does not subsume all other cyber asset types.
- Considering a lower bound to the term ‘adverse’ in “adverse impact”.
- Clarifying the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that “N-1 contingency” is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope.

B) Network and Externally Accessible Devices – V5TAG recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:
   - The 4.2.3.2 exemption phrase “between discrete Electronic Security Perimeters.” When there is not an ESP at the location, consider clarity that the communication equipment considered out of scope is the same communication equipment that would be considered out of scope if it were between two ESPs.

2 Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

Yes:
No: X

Comments:

3 Are there any other concerns with this SAR that haven’t been covered in previous questions?

Yes: X
No:

Comments*:*

Seattle would like to see the SAR address three additional areas:

A) Clarify those standards and parts where the requirement applies solely to the applicable BES Cyber System, those standards and parts where the requirement applies solely to individual BES Cyber Assets, those where the requirement applies to both BCS and BCA or to either at the option of the responsible entity, and those where the requirement applies to both BCS and BCA or to either depending on the circumstances and configuration.

B) Clarify application of CIP-002-5, in particular the R1 identification of BES Cyber Systems and their association with specific types of assets (small “a”). The linkage is inconsistent: for High impact rating it is any “BCS located at and used by” a Control Center whereas for Medium

impact rating it is any "BCS associated with any of the following," the "following" being a mixed-bag collection of capital "F" Facilities, various systems or groups of Elements, specifically defined terms such as Control Center and Special Protection System, and undefined common-language concepts such as "generation" and "BES reactive resource." Please also clarify the intent of "used by" and "associated with." Does "used by" mean "essential to the operation of," "involved in the operation of," or something else? Does "associated with" combine the concepts of "used by and located at," or would it be sufficient to be either "situated at the physical location of" or "used by"? The present language creates considerable confusion.

C) *Clarify the application of Intermediate System, as discussed by Salt River Project in their comments. Seattle supports Salt River's position and analysis.*

Seattle also supports the position that Florida Municipal Power Authority as they submitted in their comments.

Comments received from Kara Douglas – NRG

Questions

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

   Yes:
   No: X
   Comments:

   A) Please consider the definition of Cyber Asset and clarify the intent of the term "Programmable" through consideration of whether a device is merely configurable, its executable code is not field upgradable or field Programmable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc. (which relates to upgrading the executable in the Programmable code and the ability to field program the configuration)

   B) In relation to the terms: "adverse impact" and "control center", NRG proposes that when addressing TO and TOP Control Center functional obligations in CIP-002-5.1 Attachment 1, it also consider addressing similar issues facing Generator Owners (GO) and Generator Operators (GOP). There are GOP "control centers" that do not have traditional control capabilities over generator breakers or output but simply verbally direct generator actions. In this case it is the GOs that perform the actual output changes and breaker operation. Clarifying GO/GOP obligations in tandem with proposed TO/TOP clarification for determining impact is a step forward.

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

Yes:
No: X
Comments:

3. Are there any other concerns with this SAR that haven't been covered in previous questions?

   Yes:
   No: X
   Comments:

Comments received from Marc Donaldson, Tacoma Power

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

   Yes:

   No: X

   Comments: Tacoma Power suggests the following scope changes:

   - SDT should clarify CIP-005 R1 Part 1.5 with respect to encrypted communications, either in the G&TB or, directly within the requirement language.
   - SDT could provide clarity on CIP-002 eliminating ambiguous language ("Facility" vs. "facility" & "location") etc.
   - SDT should clarify whether CIP Exceptional Circumstance exception applies to CIP-004 R3 (PRA). Within the Guidelines and Technical Basis, there is this clarifier "except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response." We suggest the SDT include an exception for CIP Exceptional Circumstance specifically within the requirement language.

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

   Yes:

No: X

Comments:

3. Are there any other concerns with this SAR that haven't been covered in previous questions?

   Yes:

   No: X

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard(s):	Modifications to CIP Standards		
Date Submitted:	June 1, 2016		
SAR Requester Information			
Name:	Stephen Crutchfield		
Organization:	NERC		
Telephone:	609-651-9455	E-mail:	Stephen.Crutchfield@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard		☒ Withdrawal of existing Standard	
☒ Revision to existing Standard		☐ Urgent Action	

SAR Information
Purpose (Describe what the standard action will achieve in support of Bulk Electric System reliability.):
The purpose of this project is to (1) consider the Version 5 Transition Advisory Group (V5TAG) issues identified in the *CIP V5 Issues for Standard Drafting Team Consideration* (V5TAG Transfer Document) and (2) address the Federal Energy Regulatory Commission (Commission) directives contained in Order 822. These revisions will increase reliability and security to the Bulk-Power System (BPS) by enhancing cyber protection of BPS facilities.
Industry Need (What is the industry problem this request is trying to solve?):
The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by the existing standard drafting team (SDT) for the CIP Reliability Standards.

SAR Information

The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that the SDT consider them in future development activity.

On January 21, 2016, the Commission issued Order No. 822 approving revisions to the CIP version 5 standards and also directing NERC to develop modifications to address:

- Protection of transient electronic devices used at low-impact BES Cyber Systems;
- Protections for communication network components between control centers; and
- Refinement of the Low Impact External Routable Connectivity (LERC) definition.

The Commission did not provide a date by which the modifications for transient devices or communication networks must be completed. For the LERC definition, however, the Commission directed that NERC submit the modification within one year of the effective date of Order No. 822 (March 31, 2017).

Brief Description (Provide a paragraph that describes the scope of this standard action.)

The proposed project will consider the issues raised by the V5TAG in the V5TAG Transfer Document and will address the Commission directives in Order No. 822 through modifications to the CIP standards. The work will include development of Violation Risk Factors, Violation Severity Levels, and an Implementation Plan for the modified standards and will meet the deadlines established by the Commission in Order No. 822.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

As stated above, the purpose of this project is to consider the V5TAG issues in the initial transfer document V5TAG Transfer Document and address the Commission directives contained in Order 822. For the directive on the LERC definition, the project is to respond within the deadline required in the order.

As noted above, the V5TAG identified specific issues with the CIP V5 standards. The V5TAG drafted the V5TAG Transfer Document to formally recommend that the SDT address these issues during standards development to consider whether modifications can be made to the standard language. As outlined in the V5TAG Transfer Document, the specific issues are as follows:

- Cyber Asset and BES Cyber Asset (BCA) Definitions – as foundational definitions within the CIP V5 standards, the understanding of Cyber Asset and BCA terms impacts the scope of the applicable requirements. The V5TAG recommends the following enhancements:
  - Clarify the intent of “programmable” in Cyber Asset.
  - Clarify and focus the definition of “BES Cyber Asset” including:
    - Focusing the definition so that it does not subsume all other cyber asset types.
    - Considering a lower bound to the term ‘adverse’ in “adverse impact”.

SAR Information

- Clarifying the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that "N-1 contingency" is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope.

- Network and Externally Accessible Devices – V5TAG recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:
  - The 4.2.3.2 exemption phrase "between discrete Electronic Security Perimeters"
  - The meaning of the word 'associated' in the ERC definition.
  - The applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section.
  - The IRA definition placement of the phrase "using a routable protocol" in the definition and with respect to Dial-up Connectivity.
  - The Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."
- Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations – V5TAG is aware of multiple interpretations of the language "used to perform the functional obligation of" in CIP-002-5.1 Attachment 1, section 2.12 and recommends clarification of:
  - The applicability of requirements on a TO Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.
  - The definition of Control Center.
  - The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.
- Virtualization – The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider the CIP V5 standards and the associated definitions regarding permitted architecture and the security risks of virtualization technologies.

The SDT shall also address the Order No. 822 directives by developing modifications to requirements in CIP standards and the definition of LERC. The Commission directed the following:

- *Per paragraph 32, "...we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards."*

SAR Information
• *Per paragraph 53, "…the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."* • *Per paragraph 73, "…the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule…."* In addition, the SDT will review and address the CIP V5 requirements for CIP Exceptional Circumstances exceptions. Finally, the SDT will review the Guidelines and Technical Basis sections of the CIP V5 standards and adjust where appropriate as well as correct any grammatical, punctuation, and/or formatting errors, and make other errata changes to the CIP V5 standards, as necessary.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.

Reliability Functions	
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒ Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐ Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐ Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐ Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐ Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒ Transmission Owner	Owns and maintains transmission facilities.
☒ Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒ Distribution Provider	Delivers electrical energy to the End-use customer.
☒ Generator Owner	Owns and maintains generation facilities.
☒ Generator Operator	Operates generation unit(s) to provide real and Reactive Power.
☐ Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐ Market Operator	Interface point for reliability functions with commercial functions.
☐ Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles		
Applicable Reliability Principles (Check all that apply).		
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.	
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and Reactive Power supply and demand.	
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.	
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.	
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.	
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.	
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.	
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.	
Does the proposed Standard comply with all of the following Market Interface Principles?		Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.		YES
2. A reliability standard shall neither mandate nor prohibit any specific market structure.		YES
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.		YES
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.		YES

Related Standards	
Standard No.	Explanation

Related Standards	

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
FRCC	
MRO	
NPCC	
RF	
SERC	
SPP RE	
Texas RE	
WECC	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard(s):	Modifications to CIP Standards		
Date Submitted:	~~March 9~~June 1, 2016		
SAR Requester Information			
Name:	Stephen Crutchfield		
Organization:	NERC		
Telephone:	609-651-9455	E-mail:	Stephen.Crutchfield@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard		☒ Withdrawal of existing Standard	
☒ Revision to existing Standard		☐ Urgent Action	

SAR Information
Purpose (Describe what the standard action will achieve in support of Bulk Electric System reliability.):
The purpose of this project is to (1) consider the Version 5 Transition Advisory Group (V5TAG) issues identified in the *CIP V5 Issues for Standard Drafting Team Consideration* (V5TAG Transfer Document) and (2) address the Federal Energy Regulatory Commission (Commission) directives contained in Order 822. These revisions will increase reliability and security to the Bulk-Power System (BPS) by enhancing cyber protection of BPS facilities.
Industry Need (What is the industry problem this request is trying to solve?):
The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP ~~version 5~~V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by the existing standard drafting team (SDT) for the CIP Reliability Standards.

SAR Information

The V5-TAG developed the V5TAG Transfer Document to explain the issues and recommend that the SDT consider them in future development activity.

On January 21, 2016, the Commission issued Order No. 822 approving revisions to the CIP version 5 standards and also directing NERC to develop modifications to address:

- Protection of transient electronic devices used at low-impact BES Cyber Systems;
- Protections for communication network components between control centers; and
- Refinement of the Low Impact External Routable Connectivity (LERC) definition.

The Commission did not provide a date by which the modifications for transient devices or communication networks must be completed. For the LERC definition, however, the Commission directed that NERC submit the modification within one year of the effective date of Order No. 822 (March 31, 2017).

Brief Description (Provide a paragraph that describes the scope of this standard action.)

The proposed project will consider the issues raised by the V5TAG in the V5TAG Transfer Document and will address the Commission directives in Order No. 822 through modifications to the CIP standards. The work will include development of Violation Risk Factors, Violation Severity Levels, and an Implementation Plan for the modified standards and will meet the deadlines established by the Commission in Order No. 822.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

As stated above, the purpose of this project is to consider the V5TAG issues in the initial transfer document V5TAG Transfer Document and address the Commission directives contained in Order 822. For the directive on the LERC definition, the project is to respond within the deadline required in the order.

As noted above, the V5TAG identified specific issues with the CIP V5 standards. The V5TAG drafted the V5TAG Transfer Document to formally recommend that the SDT address these issues during standards development to consider whether modifications can be made to the standard language. As outlined in the V5TAG Transfer Document, the specific issues are as follows:

- Cyber Asset and BES Cyber Asset (BCA) Definitions – as foundational definitions within the CIP V5 standards, the understanding of Cyber Asset and BCA terms impacts the scope of the applicable requirements. The V5TAG recommends the following enhancements:
    - Clarify the intent of “programmable” in Cyber Asset.
    - Clarify and focus the definition of “BES Cyber Asset” including:

SAR Information

- Focusing the definition so that it does not subsume all other cyber asset types.
- Considering a lower bound to the term 'adverse' in "adverse impact".
- Clarifying the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that "N-1 contingency" is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope.

- Network and Externally Accessible Devices – V5TAG recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:
  - The 4.2.3.2 exemption phrase "between discrete Electronic Security Perimeters"
  - The meaning of the word 'associated' in the ERC definition.
  - The applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section.
  - The IRA definition placement of the phrase "using a routable protocol" in the definition and with respect to Dial-up Connectivity.
  - The Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."
- Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations – V5TAG is aware of multiple interpretations of the language "used to perform the functional obligation of" in CIP-002-5.1 Attachment 1, section 2.12 and recommends clarification of:
  - The applicability of requirements on a TO Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.
  - The definition of Control Center.
  - The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.
- Virtualization – The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider the CIP ~~005~~ V5 standards and the associated definitions ~~of Cyber Asset and Electronic Access Point~~ regarding permitted architecture and the security risks of ~~network, server and storage~~ virtualization technologies.

The SDT shall also address the Order No. 822 directives by developing modifications to requirements in CIP standards and the definition of LERC. The Commission directed the following:

- *Per paragraph 32, "...we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by*

SAR Information
transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards." • *Per paragraph 53, "…the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."* • *Per paragraph 73, "…the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule…."* In addition, the SDT will review and address the CIP V5 requirements for CIP Exceptional Circumstances exceptions. Finally, the SDT will review the Guidelines and Technical Basis sections of the CIP V5 standards and adjust where appropriate as well as correct any grammatical, punctuation, and/or formatting errors, and make other errata changes to the CIP V5 standards, as necessary.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.

Reliability Functions	
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒ Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐ Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐ Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐ Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
~~☒~~ ☐ Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒ Transmission Owner	Owns and maintains transmission facilities.
☒ Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
~~☐~~ ☒ Distribution Provider	Delivers electrical energy to the End-use customer.
☒ Generator Owner	Owns and maintains generation facilities.
☒ Generator Operator	Operates generation unit(s) to provide real and Reactive Power.
☐ Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐ Market Operator	Interface point for reliability functions with commercial functions.
☐ Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles		
Applicable Reliability Principles (Check all that apply).		
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.	
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and Reactive Power supply and demand.	
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.	
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.	
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.	
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.	
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.	
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.	
Does the proposed Standard comply with all of the following Market Interface Principles?		Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.		YES
2. A reliability standard shall neither mandate nor prohibit any specific market structure.		YES
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.		YES
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.		YES

Related Standards	
Standard No.	Explanation

Related Standards	

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
FRCC	
MRO	
NPCC	
RF	
SERC	
SPP RE	
Texas RE	
WECC	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards Standards Authorization Request (SAR)

Do not use this form for submitting comments. Use the electronic form to submit comments on the **Project 2016-02 Modifications to CIP Standards SAR**. The electronic comment form must be submitted by **8 p.m. Eastern, Thursday, June 30, 2016**.

Additional information about this project is available on the Project 2016-02 Modifications to CIP Standards page. If you have questions, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

Background Information

On January 21, 2016, the Commission issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards,* approving seven CIP Reliability Standards and new or modified definitions. On March 9, 2016, the NERC Standards Committee accepted the Standards Authorization Request (SAR) and authorized the posting of the Modifications to CIP Standards SAR. It was posted for a 30-day informal comment period March 23 – April 21, 2016. Based on the comments received, the Standard Drafting Team (SDT) made minor revisions to the SAR which will be posted for an additional 30-day informal comment period.

It was noted in the comments received on the SAR that the Virtualization issue involved more than just CIP-005 standards and the defined terms Cyber Asset and Electronic Access Point. To correct this, the SDT revised the sentence to: "Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider ~~CIP-005 and the definitions of Cyber Asset and Electronic Access Point~~ the CIP V5 standards and the associated definitions regarding permitted architecture and the security risks of ~~network, server and storage~~ virtualization technologies."

Other commenters suggested that the SDT include provisions to address CIP Exceptional Circumstances. A sentence was added to the SAR to include this topic: "In addition, the SDT will review and address the CIP V5 requirements for CIP Exceptional Circumstances exceptions."

A sentence was also added to the SAR allowing the SDT to make errata changes to the standards as necessary and to correct grammatical, punctuation and/or formatting errors in the V5 Standards: "Finally, the SDT will review the Guidelines and Technical Basis sections of the CIP V5 standards and adjust where appropriate as well as correct any grammatical, punctuation, and/or formatting errors, and make other errata changes to the CIP V5 standards, as necessary."

In the previous version of the SAR, the Transmission Service Provide (TSP) Reliability Function was checked as an applicable function. The TSP is not applicable under the CIP standards and this function was corrected by unchecking the TSP Reliability Function in this version of the SAR. Similarly, the Distribution

Provider (DP) Reliability Function was left unchecked in the original SAR. The CIP Standards apply to the DP, so this was corrected by checking the DP Reliability Function in this version of the SAR.

Questions

1. The CIP SDT revised the SAR based on the comments received in the previous posting as noted above. Do you agree with these revisions to the SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

   Yes:

   No:

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP V5 Issues for Standard Drafting Team Consideration

September 15, 2015

From experience in the V5 Transition Study and the on-going implementation efforts, the CIP Version 5 Transition Advisory Group (V5TAG) identified specific issues with the CIP Version 5 standard language that caused difficulty in implementation of the requirements. In many cases, the V5TAG members found that select language within the CIP Version 5 standards may be understood in multiple ways. These interpretations appear to go beyond the intended flexibility of the standard language that is necessary to accommodate the diverse nature of facts and circumstances across the electric sector. At this time, the V5TAG proposes the following issues to be addressed by the CIP V5 Revisions drafting team (SDT) or other appropriate team for standards development:

- **Cyber Asset and BES Cyber Asset definitions**

  The foundational definition for the CIP Version 5 standards is 'Cyber Assets.' When Cyber Assets meet a threshold of Bulk Electric System (BES) impact they become 'BES Cyber Assets (BCA)' which are grouped, by a Responsible Entity, into 'BES Cyber Systems (BCS).' Viewing BCAs too broadly can lead to many thousands of devices in the typical utility becoming an administrative burden for which few if any cyber security controls can actually be applied or where there is limited associated cyber security risk. Vast amounts of effort would be expended for these types of cyber assets to track and document their lack of capability for even the most basic cyber security controls. Viewing BCAs too narrowly could lead to missing consideration of devices that have a sufficient level of cyber capability and risk impact.

  The SDT should consider the definition of Cyber Asset and clarify the intent of "programmable" by considering such factors as if a device is merely configurable, its executable code is not field upgradable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc.

  The SDT should consider clarifying and focusing the definition of "BES Cyber Asset" including:

  a. Focusing the definition so that it does not subsume all other cyber asset types. Protected Cyber Assets (PCA), by nature of being on the same network, can have some form of adverse impact if misused. Electronic Access Control or Monitoring Systems (EACMS) if misused or unavailable can have some form of adverse impact. This can result in a "hall of

mirrors" effect where everything in or that creates an Electronic Security Perimeter (ESP) also meets the BCA definition.

b. Considering if there is a lower bound to the term 'adverse' in "adverse impact". For example, is the focus of a typical generating unit the servers and operator human machine interfaces (HMI) and controller cabinets and Programmable Logic Controllers (PLCs) or is it the thousands of individual sensors and transmitters throughout the plant?

c. Clarify the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that "N-1 contingency" is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope.

- **Network and Externally Accessible Devices (ERC, ESP, IRA)**

  The SDT should consider the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:

  a. Clarify the 4.2.3.2 exemption phrase "between discrete Electronic Security Perimeters." When there is not an ESP at the location, consider clarity that the communication equipment considered out of scope is the same communication equipment that would be considered out of scope if it were between two ESPs.

  b. The word 'associated' in the ERC definition is unclear in that it alludes to some form of relationship but does not define the relationship between the items. Striking 'associated' and defining the intended relationship would provide much needed clarity.

  c. Review of the applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section. As well, consider the interplay between IRA and ERC.

  d. Clarify the IRA definition to address the placement of the phrase "using a routable protocol" in the definition and clarity with respect to Dial-up Connectivity.

  e. Address the Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."

- **Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations**

  CIP-002-5.1 Attachment 1 – Impact Reliability Criteria, sections 1.1, 1.2, 1.3, 1.4, 2.11, 2.12, and 2.13 employ the language "used to perform the functional obligation of", and then lists the functional registration. It was intended that this caveat would capture entities that perform obligations of a specific registered function, whether they are registered for that function or not. However, this language has caused confusion, especially in section 2.12 concerning TOP Control Centers. The term "functional obligation" may be interpreted to have different meaning in a variety of situations.

One interpretation is for the defined term Control Center to be strictly associated with the Balancing Authority (BA), Generator Operator (GOP), Reliability Coordinator (RC), and Transmission Operator (TOP) functional registrations, and that control rooms or dispatch centers owned and operated by Transmission Owners (TOs) with control of limited BES facilities would be excluded. A second interpretation may expand or contract the applicability of the Control Center designation, based on criteria that may not take into consideration overall risk to reliable operations of the BES.

Early analysis found the potential for TOs (not Registered as TOPs) that only operate limited breakers to be pulled in as medium impact Control Centers, even if the few Facilities they control are low impact. (For example, an entity with one 161kV breaker in one substation and a second 161kV breaker in a different substation, both breakers associated with low impact Facilities.) As currently written, low impact Control Centers are to be identified per criteria 3.1 and could be commensurate with risk for these scenarios.

Areas for the SDT to address are:

a. CIP-002-5.1, Attachment 1 Control Center criteria for additional clarity and for possible revisions related to TOP or TO Control Centers performing the functional obligations of a TOP, in particular for small or lower-risk entities. A potential revision could be a size for criteria 2.12, Control Centers performing the functional obligations of a TOP.
b. Clarify the applicability of requirements on a TO Control Center that perform the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES. Review the corresponding Guidelines and Technical Basis of CIP-002-5.1, specifically: the "CIP-002-5" section paragraph starting with "Responsibility for the reliable operation of the BES is spread across all Entity Registrations"; the table following that paragraph; the "High Impact Rating (H)" section; and the criterion bullets for Control Centers under the "Medium Impact Rating (M)" section.
c. The definition of Control Center (if pursued, recognize possible impacts on operations and planning standards and/or glossary terms that include 'Control Center', for example, the revised Glossary term for "System Operator" to be effective July 1, 2016).
d. The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.

- **<u>Virtualization</u>**

  The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration.

The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies.

The transition to CIP Version 5 continues as the compliance deadline of April 1, 2016 approaches. The V5TAG continues to discuss challenging issues being undertaken during the on-going implementation. The group may find additional issues to transfer to the SDT for consideration.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards Standards Authorization Request

Informal Comment Period Open through June 30, 2016

Now Available

A 30-day informal comment period for the **Project 2016-02 Standards Authorization Request (SAR)**, is open through **8 p.m. Eastern, Thursday, June 30, 2016**.

Commenting

Use the electronic form to submit comments on the SAR. If you experience any difficulties in using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 8 p.m. Eastern).

Next Steps

The drafting team will review all responses received during the comment period and determine the next steps of the project

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards SAR June 2016
Comment Period Start Date:	6/1/2016
Comment Period End Date:	6/30/2016
Associated Ballots:	

There were 21 sets of responses, including comments from approximately 21 different people from approximately 21 companies representing 8 of the Industry Segments as shown in the table on the following pages.

Questions

1. The CIP SDT revised the SAR based on the comments received in the previous posting as noted above. Do you agree with these revisions to the SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
MRO	Emily Rousseau	1,2,3,4,5,6	MRO	MRO-NERC Standards Review Forum (NSRF)	Joe Depoorter	Madison Gas & Electric	3,4,5,6	MRO
					Chuck Lawrence	American Transmission Company	1	MRO
					Chuck Wicklund	Otter Tail Power Company	1,3,5	MRO
					Dave Rudolph	Basin Electric Power Cooperative	1,3,5,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Jodi Jenson	Western Area Power Administration	1,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Mahmood Safi	Omaha Public Utility District	1,3,5,6	MRO
					Shannon Weaver	Midwest ISO Inc.	2	MRO
					Mike Brytowski	Great River Energy	1,3,5,6	MRO
					Brad Perrett	Minnesota Power	1,5	MRO
					Scott Nickels	Rochester Public Utilities	4	MRO
					Terry Harbour	MidAmerican Energy Company	1,3,5,6	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,4,5,6	MRO

					Tony Eddleman	Nebraska Public Power District	1,3,5	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
BC Hydro and Power Authority	Patricia Robertson	1,2,3,5		BC Hydro	Patricia Robertson	BC Hydro and Power Authority	1	WECC
					Venkataramakrishnan Vinnakota	BC Hydro and Power Authority	2	WECC
					Pat G. Harrington	BC Hydro and Power Authority	3	WECC
					Clement Ma	BC Hydro and Power Authority	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7	NPCC	RSC	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Mark J. Kenny	Eversource Energy	1	NPCC
					Gregory A. Campoli	NY-ISO	2	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					David Ramkalawan	Ontario Power Generation	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC

					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Brian Shanahan	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					Michael Forte	Con-Edison	1	NPCC
					Kelly Silver	Con-Edison	3	NPCC
					Peter Yost	Con-Edison	4	NPCC
					Sean Bodkin	Dominion	4	NPCC
					Silvia Parada Mitchell	NextEra Energy	4	NPCC
					Brian O'Boyle	Con-Edison	5	NPCC
					Kathleen M. Goodman	ISO-NE	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
Colorado Springs Utilities	Shannon Fair	1,3,5,6		Colorado Springs Utilities	Kaleb Brimhall	Colorado Springs Utilities	5	WECC
					Charlie Morgan	Colorado Springs Utilities	3	WECC
					Shawna Speer	Colorado Springs Utilities	1	WECC
					Shannon Fair	Colorado Springs Utilities	6	WECC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Jason Smith	Southwest Power Pool Inc	2	SPP RE

					Kim VanBrimer	Southwest Power Pool Inc	2	SPP RE
					John Allen	City Utilities of Springfield	1,4	SPP RE
					Mike Buyce	City Utilities of Springfield	1,4	SPP RE
					Paul Mehlhaff	Sunflower Electric Power Corporation	1	SPP RE
					TARA Lightner	Sunflower Electric Power Corporation	1	SPP RE
ACES Power Marketing	Warren Cross	1,3,4,5	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Brazos Electric Power Cooperative, Inc.	BREC	1,5	Texas RE
					Western Farmers Electric Cooperative	WFEC	1,5	SPP RE
					Old Dominion Electric Cooperative	ODEC	3,4	SERC
					Golden Spread Electric Cooperative	GSEC	5	SPP RE
					Prairie Power, Inc.	PPI	1,3	SERC
					Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF

1. The CIP SDT revised the SAR based on the comments received in the previous posting as noted above. Do you agree with these revisions to the SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

Bob Reynolds - 10	
Answer	No
Document Name	
Comment	

The SPP RE respectfully submits the following two comments to the Project 2016-02 Standards Authorization Request: (1) Reference the comments submitted by the SPP Regional Entity (SPP RE) April 2016. In those comments, the SPP RE pointed out that Tie Line and other Transmission line flow meters appear to have been unintentionally excluded from consideration under CIP-002-5.1, Impact Rating Criterion 2.5. This significant issue does not appear to have been included in the revised SAR. The original SPP RE comment is restated here: "Impact Rating Criterion 2.5 excludes consideration of BES Cyber Assets associated with Transmission lines through its use of "operating between 200 kV and 499 kV at a single station or substation" language. In the instance where the tie line or other flow meter is associated with a Transmission Line operated between 200 and 499 KV in a substation that satisfies the qualifications of Impact Rating Criterion 2.5, the meter will be excluded and not be categorized as Medium Impacting. Additionally, some entities are proffering the argument that the flow meter is not a BES Cyber Asset because its loss or misuse will not affect the reliable operation of the Transmission Facilities in the substation where the meter resides, overlooking the impact the loss of meter information may have on Control Center operations including ACE calculation, security-constrained generation dispatch, AGC, and Situational Awareness. An additional Criterion, specific to Transmission line flow meters, may be required to address this issue." (2) The SPP RE notes that the revised SAR still makes no mention of the consideration of submitted and outstanding Requests for Interpretation. NERC staff has stated publicly that the RFIs would be addressed by the Standards Drafting Team. The SPP RE is aware that at least one of the issues discussed in the April 2016 comments to the SAR has been formally submitted as a Request for Interpretation. To fail to consider outstanding RFIs in the course of modifying the CIP Standards under this SAR would be a missed opportunity to address significant confusion regarding the expectations of the Requirements under question.

Likes 0	
Dislikes 0	

Response

Mike Smith - 1,3,5,6	
Answer	No
Document Name	
Comment	

For virtualization, Manitoba Hydro does not agree with NERC prescribing specific system architecture, technologies or designs. SDT should continue to focus on identifying requirements to meet specific objectives for the virtualization.

Manitoba Hydro agrees with adding more CIP V5 requirements exceptions for CIP Exceptional Circumstance.

Likes 0	
Dislikes 0	

Response	
Emily Rousseau - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)	
Answer	No
Document Name	
Comment	
The NSRF agrees with the drafting team's addition of "reviewing and addressing the CIP V5 requirements for CIP Exceptional Circumstances exceptions" to the SAR. However, we request clarification on the scope of Guidelines and Technical Basis sections that may be changed with updates to the associated Standards within this project. We believe that addressing all CIP V5 Guidelines and Technical Basis sections within the scope of this revision may make the project unwieldy as it already contains a substantial scope of work to address FERC directives. We suggest that only Guidelines and Technical Basis sections related to standards language updates should be addressed within the scope of this project.	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - 1,2,3,5, Group Name BC Hydro	
Answer	No
Document Name	
Comment	

CIP-002-5.1

A) The topic of adverse impact should provide more clarity on the real-time requirement as well.

B) Per Medium Impact criterion 2.3 for generation resources, need further clarity on the extent of planning horizon > 1 year contingencies to consider regarding the determination of BES Adverse Reliability Impacts to a given Interconnection. The Guidelines and Technical basis of CIP-002-5.1 reference as an example, TPL-003 Category C3 contingency system studies but otherwise, there is no lower or upper limit indicated regarding the depth of contingencies to be considered. The limit is currently subjective for Transmission Planners and Planning Coordinators.

Furthermore, per the definition of Adverse Reliability Impact, there is direct reference to impacts on a given Interconnection but it is not clear whether this is only considering inter-tie paths or general BES impacts beyond a specific BES location (i.e. generation plant or substation). The Guidelines and Technical basis state only widespread impacts are to be considered instead of localized impacts but it is not clear what is considered 'widespread'.

CIP-005-5 The fundamental concepts of the intermediate system are omitted or subjective. The standards should define what the requirements are for this system, whether it is strictly a jump host (not mentioned in the standards) or can have more functionality (i.e. software installed upon it). This should be included in the 'Network and Externally Accessible Devices' section.

CIP-005-5/CIP-003-6 A clear exemption is given for low impact systems is given in CIP-003-6 Guidelines and Technical Basis (CIP-006-6 pg 28) "To future-proof the standards, and in order to avoid future technology issues, the definitions specifically exclude "point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems," such as IEC 61850 messaging." The 'Network and Externally Accessible Device'"

section should address this topic for medium impact BCS/BCA as well. These technologies are not limited to low impact systems and guidance should be provided.

CIP-007-5: Regarding security patch applications and cyber vulnerability assessments:

- Certain legacy devices (i.e. HMIs, PLCs, etc.) can be in a "fragile" state and are at high-risk regarding the application of software updates, which include cyber security related updates. There is a demonstrable risk in breaking their functionality which can have an adverse impact on the BES as the only solution is to replace the device entirely or at best, perform a complete reset of the device. This is mainly due to bugs that could be introduced by vendors through their patches (not enough regression testing done by the vendors) and for which even testing prior to implementation in a production environment may not identify all such bugs prior to implementation. Recommend providing guidance around how to handle the application of cyber security patches to these "fragile" devices and to potentially not mandate security patch applications in all cases where there may be demonstrable evidence of adverse BES impact.

- Further guidance is required within the Guidelines and Technical basis on the exact difference between a 'paper' exercise cyber vulnerability assessments (CVA) and 'active' CVA with respect to Medium Impact facilities and the extent an entity is expected to go to achieve this. It has been communicated by Regional Entities' audit approach that paper scans must incorporate some active component to pull configuration settings, etc. from a device for analysis. For legacy devices (namely firmware devices), these active component scans can also pose a risk in breaking the functionality of said devices, which can cause adverse impact to the BES. Recommend including guidance around how to handle CVAs pertaining to these firmware devices without potentially breaking their functionality.

Likes 0	
Dislikes 0	

Response

Chris Mattson - 1,3,4,5,6

Answer	No
Document Name	

Comment

Tacoma asks that the SDT consider removing the final two sentences from the last paragraph of CIP-005-5, Guidelines and Technical Basis, Section 4 – Scope and Applicability of the CIP Cyber Security Standards, Requirement R1. These are shown in bold below for identification:

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 misconfigured. The Order makes clear that this is not simply 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.***

Tacoma is asking the SDT to consider that there are other methods and technologies for detecting malicious traffic in addition to deep packet inspection. This change to the G&TB would make the standard more consistent with the language in FERC Order No. 706, Paragraph 501 which indicates that it is not the commission's intent to mandate any specific mechanism to be the second security measure. The language from the FERC order is shown below for reference and the pertinent language is shown in bold:

Paragraph 501. In response to SDG&E and Entergy, in stating that the placement of security measures in front of systems provides a layer of protection for those systems, the Commission was not giving priority to "in front" measures. In fact, the Commission acknowledged in the CIP NOPR that defense

in depth measures are generally integrated within and constitute part of a system or program. In commenting that defense in depth measures may also be effectively placed in front of a system, the Commission intended only to acknowledge that there are multiple ways to implement a defense in depth strategy. ***The Commission is not mandating any specific mechanism to be the second security measure. We are also not requiring uniformity of security measures, only that each responsible entity have at least two security measures unless it is not technically feasible to do so.*** *The revised CIP Reliability Standard should allow enough flexibility for a responsible entity to take into account each site's specific environment. The Commission believes that this, in conjunction with the allowance of technical feasibility exceptions, alleviates FPL Group's concern that the Commission's proposal is a "one size fits all" approach.*

Also, the SDT should clarify CIP-005 R1 Part 1.5 with respect to encrypted communications either in the G&TB or directly within the requirement language. It important that the SDT clarify how to detect malicious communications when the communications includes encrypted information that is not readily decrypted to allow inspection.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

.

Although Seminole concurs with all items currently listed in the draft Standards Authorization Request, Seminole recommends that additional items should be included in the SAR. Seminole thanks the SAR team for addressing our previous comments, in addition to those of others, related to Exceptional Circumstances and the Guidelines and Technical Basis.

While the changes addressed are necessary to address mandatory requirements from FERC, this SAR does not address the fundamental deficiencies in the current CIP standards. Until these fundamental issues are addressed, the electric sector will continue to struggle implementing the current standard, be faced with inefficiencies in the standard that do not improve cyber and physical security, and have difficulty using new and improved capabilities in a rapidly evolving marketplace.

Seminole recommends adding the following items to the SAR:

1. Update CIP-002 Requirements and the Guidelines and Technical Basis section to clarify the expectations in complying with this standard. Update evidence requirements to make clear the expectations of the standard. Clarify attachment 1 to address V5TAG Lessons Learned and FAQs. Resolve issues in the Guidelines and Technical Basis that are inconsistent with the definition of BES Cyber Asset and BES Cyber System.

2. The SDT will review applicable Standards and Requirements to clarify the SDT's intent for management of shared Facilities when more than one Registered Entity owns Facilities inside a single asset. Interconnections within the BES and with Distribution Providers within a single asset create significant complexity for entities in some regions. This results in a need for a significant number of MOU, CFR, or JRO that both complicates compliance and the audit process.

3. The SDT will review the Measures in the CIP V5 standards and adjust where appropriate to allow an entity that provides evidence consistent with the identified measures to determine compliance if no deficiencies are identified in the provided evidence. This may include modifying measures to match the CIP Version 5 Evidence Request or by clarifying either the measures or Guidelines and Technical basis to clarify intent for adjustment of the evidence request.

Likes 0	
Dislikes 0	

Response

Julie Hall - 6

Answer	No
Document Name	

Comment

Comments: Entergy requests that more detail be provided regarding the actions that will be considered regarding CIP Exceptional Circumstances. Is more specificity regarding what constitutes a CIP Exceptional Circumstance being considered? Is more specificity regarding how to declare and document a CIP Exceptional Circumstance being considered? Will more clarity regarding standards affected by CIP Exceptional Circumstance, including a possible increase of applicable standards, be considered? Some particular questions Entergy has regarding the scope of standards affected by CIP Exceptional Circumstances include:

- CIP-004-5.1 R3 does not include the “except during CIP Exceptional Circumstances” language, yet the Guidelines and Technical Basis section states “Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response.” The language in the Guidelines and Technical Basis seems logical as it may not be feasible to validate PRA’s during a widespread emergency response (i.e. a hurricane) especially when response support is provided by many other companies and/or vendors across the country. It is requested that the “except during CIP Exceptional Circumstances” language be added to the appropriate parts of CIP-004-5.1 R3, particularly CIP-004-5.1 R3 Part 3.5.

- The “except during CIP Exceptional Circumstances” language exists in CIP-006-5 R2 Part 2.1 and Part 2.2 which states that logging and continuous escorting of visitors is not required during CIP Exceptional Circumstances. However, none of the CIP-006-5 R1 parts include the “except during CIP Exceptional Circumstances” language, which in turn requires alerting, monitoring, logging of access approved individuals. This may not be feasible during a widespread event that results in total loss of power at many sites over a widespread geographical area. It is requested that the “except during CIP Exceptional Circumstances” language be added to the appropriate parts of CIP-006-5, particularly R1 to ensure consistency across CIP-006-5.

Likes 0	
Dislikes 0	

Response

Scott Brame - 3,4,5 - SERC	
Answer	No
Document Name	
Comment	

The following comments are from my CIP SME.

• Per paragraph 73, "…the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d) (5) of the FPA, we direct NERC to develop a modification.

This is where I believe FERC's order falls short. Although, the definition for LERC needs to be improved and needs to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6. In my opinion, the requirements for low impact critical assets is incomplete. It appears like the SDT was rushed to provide requirements for low impact. Although, the SDT included some basic requirements for low impact critical assets they should have also included requirements for malware and virus protections. In addition, there should be requirements for logging and auditing of systems and system access. These requirements do not need to be as stringent and comprehensive as what is required for medium and high impact critical assets, but they should also be required for low impact critical assets.

Likes 0	
Dislikes 0	
Response	

Warren Cross - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	

Thank you for the opportunity to provide comments regarding the Standards Authorization Request (SAR) in response to FERC Directives and v5TAG recommendations. While the current SAR attempts to resolve issues around LERC, virtualization and communication protections, ACES believes the SAR doesn't adequately detail the areas of concern for LERC and fails to allow for technology advances, which may ultimately hinder industry adoption of more secure solutions to address cyber security threats.

How LERC will be defined based upon the ability to communicate and interactive communication capabilities between Low Impact Facilities that have BES Cyber Assets associated with them has yet to be fully vetted. The ability to communicate with a BES Cyber Asset isn't the same as interacting with the BES Cyber Asset. This distinction needs to be clearly defined. Another issue for Low Impact BES Cyber Systems is the need for a common definition of when serial devices are in scope and not in scope for consistent industry implementation.

Host-based security applications, advanced security threat analysis services, and cloud-based networks are not in scope for the SAR. There are mechanisms in place in the CIP standards that allow for exceptions, such as TFEs and CIP Exceptional Circumstances. ACES believes that these definitions could be expanded to include technology that exists outside of the standard to be able to be used, with approval, in order to provide the entity with a stronger defense in depth security profile.

If the drafting team proposes to modify definitions, they should consider a process that is non-prescriptive and provides flexibility for registered entities to decide how to best defend against cyber security threats based on their risk analysis. There may be significant advantages for industry to adopt new emerging security applications and cloud based security services. The CIP standards should not limit the tools or technology available to mitigate cyber security risks. We ask the drafting team to consider how the revisions to the CIP standards would allow for the power industry to match the security best practices of other industries against the latest security threats and vulnerabilities.

Thank you for your time and attention regarding this SAR.

Likes 0	
Dislikes 0	

Response

Erika Doot - 1,5

Answer	No
Document Name	

Comment

The Bureau of Reclamation agrees with the drafting team's addition of "reviewing and addressing the CIP V5 requirements for CIP Exceptional Circumstances exceptions" to the SAR. However, Reclamation requests clarification on the scope of Guidelines and Technical Basis sections that may be changed with updates to the associated Standards within this project. Reclamation believes that addressing all CIP V5 Guidelines and Technical Basis sections within the scope of this revision may make the project unwieldy as it already contains a substantial scope of work to address FERC directives. Reclamation suggests that only Guidelines and Technical Basis sections related to standards language updates should be addressed within the scope of this project.

Likes 0	
Dislikes 0	

Response

Shannon Fair - 1,3,5,6, Group Name Colorado Springs Utilities

Answer	Yes
Document Name	

Comment
CSU supports the standard dradting teams updates to the SAR.

Likes 0	
Dislikes 0	

Response

Thomas Foltz - 3,5	
Answer	Yes
Document Name	

Comment
AEP suggests that the SDT include separate balloting and commenting for Guidelines and Technical Basis throughout this project. With the development of implementation guidance, AEP is unsure whether the Guidelines and Technical Basis document should remain a part of the codified Reliability Standard. If it does, then stakeholders should have the ability to vote and comment on the contents specifically.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	

Comment
As our review group evaluated the revised SAR, we noticed that the V5TAG recommends providing clarity in the definitions of the two terms ‘External Routable Connectivity (ERC)’ and ‘Interactive Remote Access (IRA). We suggest the drafting team either develop a new SAR or modify this one in order to require the term ‘External Routable Connectivity (ERC)’ to have the acronym and revised definition updated in the NERC Glossary and also included in the Rules of Procedure (RoP) for consistency and proper alignment. Additionally, we suggest the drafting team edit the SAR to review the Rules of Procedure where the acronym (IRA), is used to refer to ‘Inherent Risk Assessment’ wheras the CIP Standards refer to a term ‘Interactive Remote Access’ but do not use an acronym. There could be confusion if an acronym is used in either document for either of these terms. We suggest not using an acronym for either term in any document. We also request clarification on why there is a specific deadline for updating the definition of LERC. As for the term ‘Low Impact External Routable Connectivity-LERC’, we suggest the drafting team edit the SAR to clarify that a revised definition will also be included in the RoP.

When clarifying the ‘lower bound’ clarification in “adverse impact”, we would appreciate a clear example (beyond the one used in the V5TAG document) that explains this concept.

We also request the SDT review or consider creating definitions or otherwise providing clarity for ‘custom software’ and the use of ‘scripts’. There are several instances of regional inconsistencies in the scope of ‘scripts’ that should be included in an entity’s baseline. Direction or clarity from this drafting team would be appreciated. Additional requirements or definitions may not be required, but guidance, rationale, or technical background would be beneficial.

Likes 0	
Dislikes 0	

Response

Stephanie Little - 1,3,5,6

Answer	Yes
Document Name	

Comment

Arizona Public Service (AZPS) appreciates the opportunity to comment on the revised SAR, and submits the following comments previously provided in response to the initial SAR. Although AZPS generally supports the scope as described in the SAR, we believe that there are additional clarifications that should be considered beyond those detailed in the FERC Oder 822 and the CIP Version 5 Transition Advisory Group (V5TAG) considerations.

AZPS believes the industry would benefit from clarification of the definition of the following terms:

- Transmission Facility – Transmission Facility is not a defined term. Although Facility is a defined term, AZPS does not believe that the Facility definition aligns with the standard’s intent. AZPS suggests that a definition be provided by the Standard Drafting Team (SDT).

- Programmable - The SDT should consider defining programmable to clarify that a device would not be included simply because it was configurable, e.g., has functionality that can be changed locally.

AZPS would also like to suggest that the SDT clarify the intent of the grouping BCAs into BCS by leveraging the logically based perimeter security controls at the Electronic Security Perimeter (ESP) as well as local, device specific security controls per each BES Cyber Asset’s (BCA) capability.

AZPS would also like to add some additional comments to the discussion in the V5TAG CIP V5 Issues for Standard Drafting Team Consideration document.

- AZPS recommends that the SDT consider not defining “adverse impact” or defining a lower bound thereof within the definition of BES Cyber Asset, but to revise the body of CIP standards and/or applicable defined terms to utilize already defined terms such as “Adverse Reliability Impact.” Such would facilitate consistency as well as clarity regarding the N-1 contingency issue and other issues regarding that term identified by the V5TAG.

- AZPS believes that when BES Cyber Assets (BCA), such as relays, RTUs, and others, are connected via serial links to IP converters and/or IP-enabled security gateways, it would be appropriate to consider those elements downstream of the security gateways as BCA that do not have External Routable Connectivity (ERC). This is appropriate because the IP- converters and/or IP-enable security gateways require authentication and provide a protocol break. AZPS believes accurate and timely guidance related to serially connected devices supports the overall goal of providing appropriate and effective cyber security controls; thus, improving reliability.

- AZPS supports the CIP V5TAG analysis regarding virtualization. Virtualization is an effective tool for utilities and consideration should be given to ensuring that flexibility is maintained. An approach should consider the required outcome rather than the specifics of how that outcome is achieved.

AZPS also notes that NERC's webpage for this SAR "Project 2016-02 Modifications to CIP Standards", as of 4/11/2016, states the following:

"Also the scope of this work will incorporate existing and future RFIs relating to the CIP-002 through CIP-011 family of standards."

AZPS does not believe any RFIs are addressed in the current SAR. We recommend updating the SAR to reference existing submitted RFIs as appropriate. Finally, AZPS recommends removal from the SAR of functional registrations that are no longer included in the Compliance Registry, e.g., Interchange Authority, Load-Serving Entity and Purchasing-Selling Entity.

Likes 0	
Dislikes 0	

Response

Ruida Shu - 1,2,3,4,5,6,7 - NPCC, Group Name RSC

Answer	Yes
Document Name	

Comment

We support the revisions to the SAR.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

BPA agrees with the revised scope of the SAR with three exceptions regarding the "Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations –" bullet and sub-bullets:

1. BPA proposes that the SDT clearly identify which function holds the compliance documentation responsibilities.
2. BPA believes the NERC Glossary definition of control center is adequate and should not be revised. The current definition maintains the distinction between control centers and substations.
3. BPA believes no clarification of the 'performs the functions of' language is needed for Attachment 1.

Likes 0	
Dislikes 0	
Response	
larry brusseau - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darin Ferguson - 1,3,5,7 - SERC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - 10	
Answer	
Document Name	
Comment	

Texas RE supports those comments suggesting that this project should identify continued areas for improvement within the existing CIP V5 Standards and avoid engaging in a wholesale “rewrite” of the CIP Standards at this point in time. Consistent with this principle, the Standards Drafting Team (SDT) has properly identified the FERC directives from Order No. 822 and the various V5 Tag recommendations as the framework upon which to base the scope of this project.

However, Texas RE believes that the SDT should also take the opportunity to address two other areas to develop a strong record and enhance regulatory certainty around the application of the new suite of CIP Standards becoming effective on July 1, 2016. First, Texas RE agrees with those comments suggesting that the Commission should consider the interaction among the various CIP Standards, including the interaction between CIP-002-5.1 and the rest of the Standards as a group. The SDT may specifically wish to address the interplay between the various bright-line impact categories in the CIP-002-5.1 Standard and the risk assessments associated with the other CIP-005 Standards.

Second, Texas RE recommends that the SDT explicitly consider and determine whether aspects of the various supporting materials associated with the CIP Standards, including a number of Lessons Learned, FAQs, and other guidance documents should be incorporated directly into the CIP Standards themselves. For example, the October 2015 CIP V5 Consolidated FAQs and Answers provided that “HVAV, UPS, and other support systems . . . will not be the focus of compliance monitoring” unless such systems are within an Electronic Security Perimeter. (p. 7). However, some HVAC and other systems may fall within the definition of a BES Cyber System and be subject, among other things, to the categorization requirements set forth in CIP-002-5.1, R1. The SDT could add clarity to the Standards by explicitly considering whether HVAC and other support systems should be (or is already) included within the BES Cyber System definition or conversely carved out of the CIP Standards in certain circumstances. This will encourage reliability and regulatory certainty by permitting entities to look to the Standard language to understand their compliance obligations, as well as produce a transparent record of the rationale underpinning a particular approach.

Changes to SAR Redlined Language

In addition to Texas RE’s suggestions regarding the scope of this project, Texas RE also suggests two additional revisions to the revised SAR language. First, the scope of the CIP Exceptional Circumstances exception language appears vague. Texas RE presumes that the SDT incorporated the recommendations from the Edison Electric Institute and others suggesting primarily that the SDT should consider whether the CIP Exceptional Circumstances exception should be added to additional CIP V5 requirements. Texas RE recommends making this more explicit by revising the SAR

language to state: “In addition, the SDT will review and address whether it is appropriate to include CIP Exceptional Circumstances exceptions within additional CIP V5 requirements.”

Second, Texas RE supports the SDT’s inclusion of language in the SAR permitting the SDT to make non-substantive changes to the Standards and Guidelines and Technical Basis sections to correct grammar, punctuation, and/or formatting errors. However, it is possible to read the proposed language to suggest that “errata” changes are somehow broader than such non-substantive revisions. Texas RE would suggest clarifying that “errata” changes to the CIP V5 Standards by inserting the word “non-substantive” in front of the word “errata” in the existing redline language.

Likes 0	
Dislikes 0	

Response

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.

Description of Current Draft

This draft of CIP-003-7 is addressing the directive issued by the Federal Energy Regulatory Commission (Commission) in paragraph 73 of Order No. 822 which reads:

> [T]he Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule approving revisions to the cybersecurity Critical Infrastructure Protection (CIP) standards.

Previously, the Guidelines and Technical Basis had approximately 10 pages of explanation and numerous reference models to describe different forms of direct vs. indirect access that could be used to determine whether Low Impact External Routable Connectivity existed and thus whether a Low Impact BES Cyber System Electronic Access Point (LEAP) was required.

In this revision, the term *Low Impact External Routable Connectivity* has been changed to *Low Impact External Routable Communication (LERC*) and simplified so that it is an attribute of a BES asset concerning whether there is routable protocol communications across the asset boundary without regard to 'direct vs. indirect' access that may occur. This greatly simplifies and clarifies the definition of LERC. It removes the dependency between the electronic access controls that may be in place and having those controls determine whether LERC exists or not. For those BES assets that have LERC, the SDT changed the requirement from requiring a LEAP to requiring electronic access controls to "permit only necessary electronic access to low impact BES Cyber Systems" (revised Attachment 1, Section 3.1) within the BES asset and expanded the Guidelines and Technical Basis with numerous examples of electronic access controls.

Given the modified definition of LERC and the proposed modifications in Reliability CIP-003-7, there is no longer a need for the NERC Glossary term Low Impact BES Cyber System Electronic Access Point (LEAP). Consequently, NERC is proposing that term for retirement.

In summary, the CIP Standard Drafting Team revised CIP-003-7, Attachments 1 and 2, Sections 2 and 3 and the associated High VSL for Requirement R2. Non-substantive errata changes were also made within the standard, including changing "ES-ISAC" to "E-ISAC".

Completed Actions	Date
Standard Authorization Request (SAR) approved	July 20, 2016
Draft 1 of CIP-003-7 posted for formal comment and initial ballot	July 21 – September 6, 2016

Anticipated Actions	Date
10-day final ballot	October, 2016
NERC Board of Trustees (BOT) adoption	November, 2016

A. Introduction

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

2. **Number:** CIP-003-7

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 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 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 SPS or RAS where the SPS or 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-003-7:

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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3 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.

4.2.3.4 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-003-7.

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single

cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls for Low Impact External Routable Communication (LERC) and Dial-up Connectivity; and

1.2.4. Cyber Security Incident response

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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1)	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1)	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 within 15 calendar	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 within 16 calendar	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) 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 BES Cyber Systems 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	months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) 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 BES Cyber Systems 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	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.2)	calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing	The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber	The Responsible Entity failed to document or implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Incident response plans according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2)	low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and	Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to implement the electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented the physical access controls for its	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented	assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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.

Version	Date	Action	Change Tracking
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 devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees.	Revised to address FERC Order 822 directive regarding definition of LERC

Attachment 1

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

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

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

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

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

Section 3. Electronic Access Controls: Each Responsible Entity shall:

3.1 Implement electronic access control(s) for LERC, if any, to permit only necessary electronic access to low impact BES Cyber System(s).

3.2 Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security

Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Attachment 2

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

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

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

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

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

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

1. Documentation, such as representative diagrams or lists of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; authenticating users; air-gapping networks; terminating routable protocol sessions on a non-BES Cyber Asset; implementing unidirectional gateways) showing that for LERC at each asset or group of assets containing low impact BES Cyber Systems, is confined only to that access the Responsible Entity deems necessary; and
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process

documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

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

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any *assets containing low impact BES Cyber Systems,* also referred to herein as BES assets, the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are

encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control

- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

Using the list of assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that addresses objective criteria for the protection of low impact BES

Cyber Systems. The protections required by Requirement R2 reflect the level of risk that misuse or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the required protections are part of a program that covers the low impact BES Cyber Systems collectively either at an asset or site level (assets containing low impact BES Cyber Systems), but not at an individual device or system level.

There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and Dial-up Connectivity, and (4) Cyber Security Incident response.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. Guidance for each of the four subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The Responsible Entity is not required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or “If you see something, say something” campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Section 3, if any. If these Cyber Assets are located within the BES asset and inherit the same controls outlined in Section 2, this can be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility in the selection of the methods used to meet the objective to control physical access to the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves, as well as physical protection of the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of access controls, monitoring controls, or

other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

The objective is to control the physical access based on need as determined by the Responsible Entity. The need can be documented at the policy level for access to the site or systems. The requirement does not obligate an entity to specify a need for each access or authorization of a user for access.

Monitoring as a physical security control can be used as a complement or an alternative to access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for *assets containing low impact BES Cyber Systems,* also referred to herein as BES assets when external routable protocol communication (LERC) or Dial-up Connectivity is present to or from the asset containing the low impact BES Cyber System(s). The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. In the case where there is no LERC or Dial-up Connectivity, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the controls that meet their operational needs while meeting the security objective of allowing only necessary electronic access to low impact BES Cyber Systems.

In essence, Responsible Entities are to determine LERC or Dial-up Connectivity for their BES assets and then, if present, document and implement electronic access control(s).

Determining LERC

The defined term Low Impact External Routable Communication (LERC) is used to avoid confusion with the term External Routable Connectivity (ERC) used for high and medium impact BES Cyber Systems as these terms are different concepts. The input to this requirement from CIP-002 is a list of assets containing low impact BES Cyber Systems, therefore LERC is an attribute of a BES asset and involves routable protocol communications to or from the BES asset (crossing the asset boundary) without regard to connectivity to Cyber Assets within the BES asset. ERC on the other hand is an attribute of an individual high or medium impact BES Cyber System and is relative to an Electronic Security Perimeter (ESP).

With LERC being a BES asset level attribute, it is used as a higher level filter to exclude from further consideration those assets containing low impact BES Cyber Systems that have no routable protocol communications to them from outside the BES asset. Responsible Entities can then concentrate their electronic access control efforts on those BES assets that do have LERC. However, this also means that LERC can exist for a BES asset even if there is no routable protocol connectivity to any low impact BES Cyber System within the BES asset.

In order to avoid future technology issues, the LERC definition specifically excludes communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between non-Control Center BES assets containing low impact BES Cyber Systems, such as IEC 61850 messaging. This does not exclude Control Center to field communication but rather excludes the communication between the intelligent electronic devices (e.g. relays) in the field. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive requirements related to this technology nor to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Determining Asset Boundary

As LERC is a BES asset level attribute, it involves a determination by the Responsible Entity of a BES asset boundary for their assets containing low impact BES Cyber Systems. This boundary will vary by BES asset type (Control Center, substation, generation resource) and the specific configuration of the BES asset. The intent is for the Responsible Entity to define the BES asset boundary such that the low impact BES Cyber System(s) that are located at the BES asset are contained within the BES asset boundary. This is strictly for determining what constitutes the BES "asset" and for determining which routable protocol communications and networks are *internal* or *inside* or *local* to the BES asset and which are *external to or outside* the BES asset. This is not an Electronic Security Perimeter or Physical Security Perimeter as defined for medium and high impact BES Cyber Systems. For the asset containing low impact BES Cyber System(s), the BES asset boundary is synonymous to the concept of a "logical border" demarcation where routable protocol communication (e.g. LERC) enters and exits the BES asset containing the low impact BES Cyber System. Some examples of ways a Responsible Entity may determine BES asset boundaries are:

- For Control Centers
  - Designated areas (room(s) or floor(s)) if the Control Center is located within a larger building.
  - A building if in a dedicated building on a shared campus.
  - The property/fence line if the Control Center is a dedicated facility on dedicated property.
- For substations, this could be the property/fence line or the control house.

- For generation resources:
  - Fossil/hydro generating facilities: This could be the property/fence line. If pumps or wells or other equipment that are part of the plant asset are outside the property line, then the BES asset boundary could expand to accommodate all that is considered part of the plant.
  - Solar farms: This could be the property line(s) or fence(s) surrounding all solar panels and interconnection facilities.
  - Wind farms: This could be the collection of individual turbines plus the equipment needed for interconnection.
  - Cogeneration facilities: This could be the identified portion of the larger plant that performs generation.

Determining Electronic Access Controls

Once a Responsible Entity has determined that LERC exists at the BES asset boundary, the Responsible Entity documents and implements its chosen electronic access control(s). The control(s) must allow only "necessary" access as determined by the Responsible Entity and they need to be able to explain the reasons for the electronic access permitted with their electronic access controls. The reasoning for the "necessary" access controls can be documented within the Responsible Entity's cyber security plan(s) or other policies or procedures associated with the electronic access controls.

Concept Diagrams

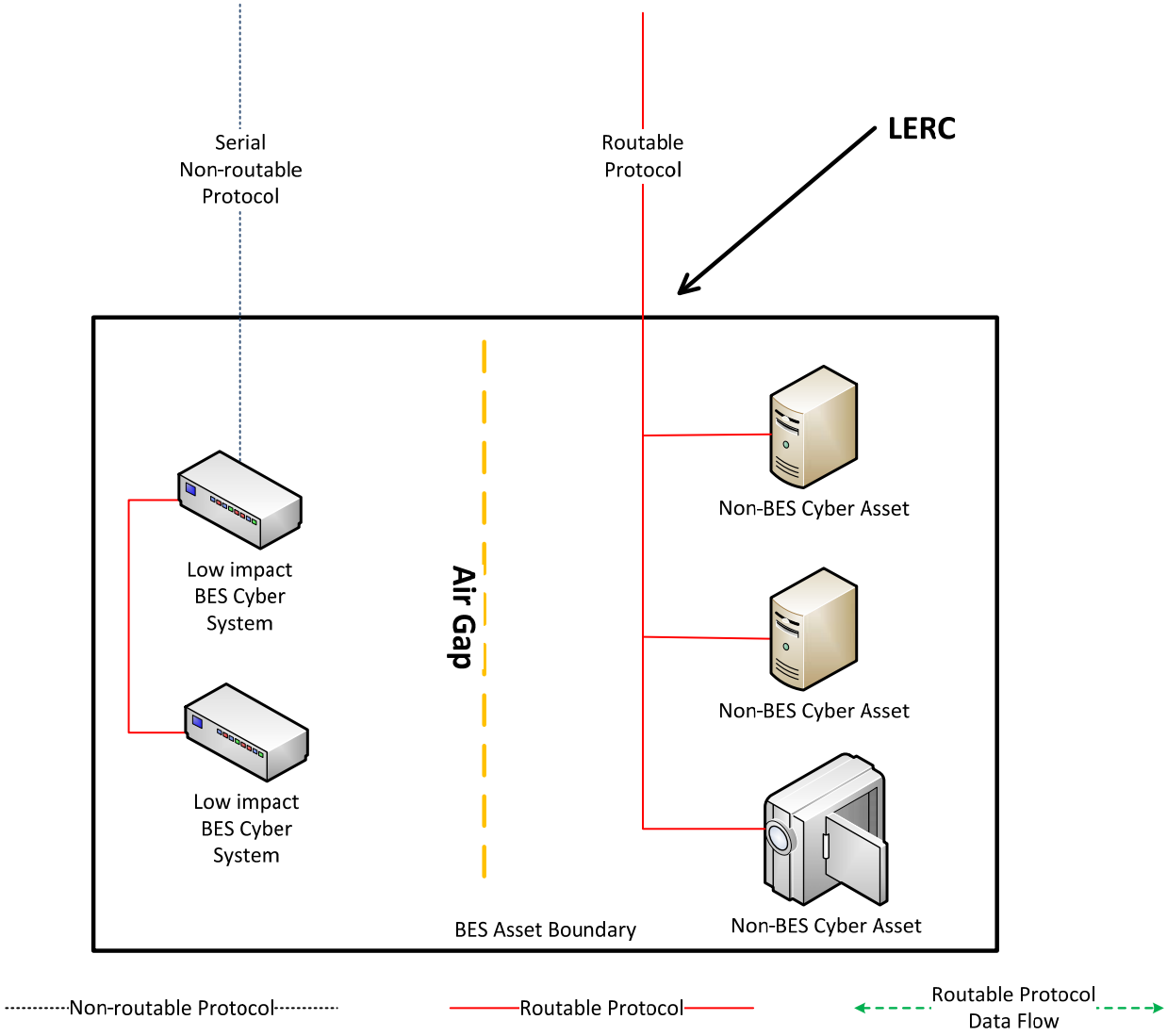
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the security objective of permitting only necessary access to low impact BES Cyber Systems must be met when there is LERC to a BES asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- LERC is present in each diagram.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.
- The term "BES Asset Boundary" is capitalized in the diagrams but it is not a defined term.

LERC Reference Model 1 – Physical Isolation

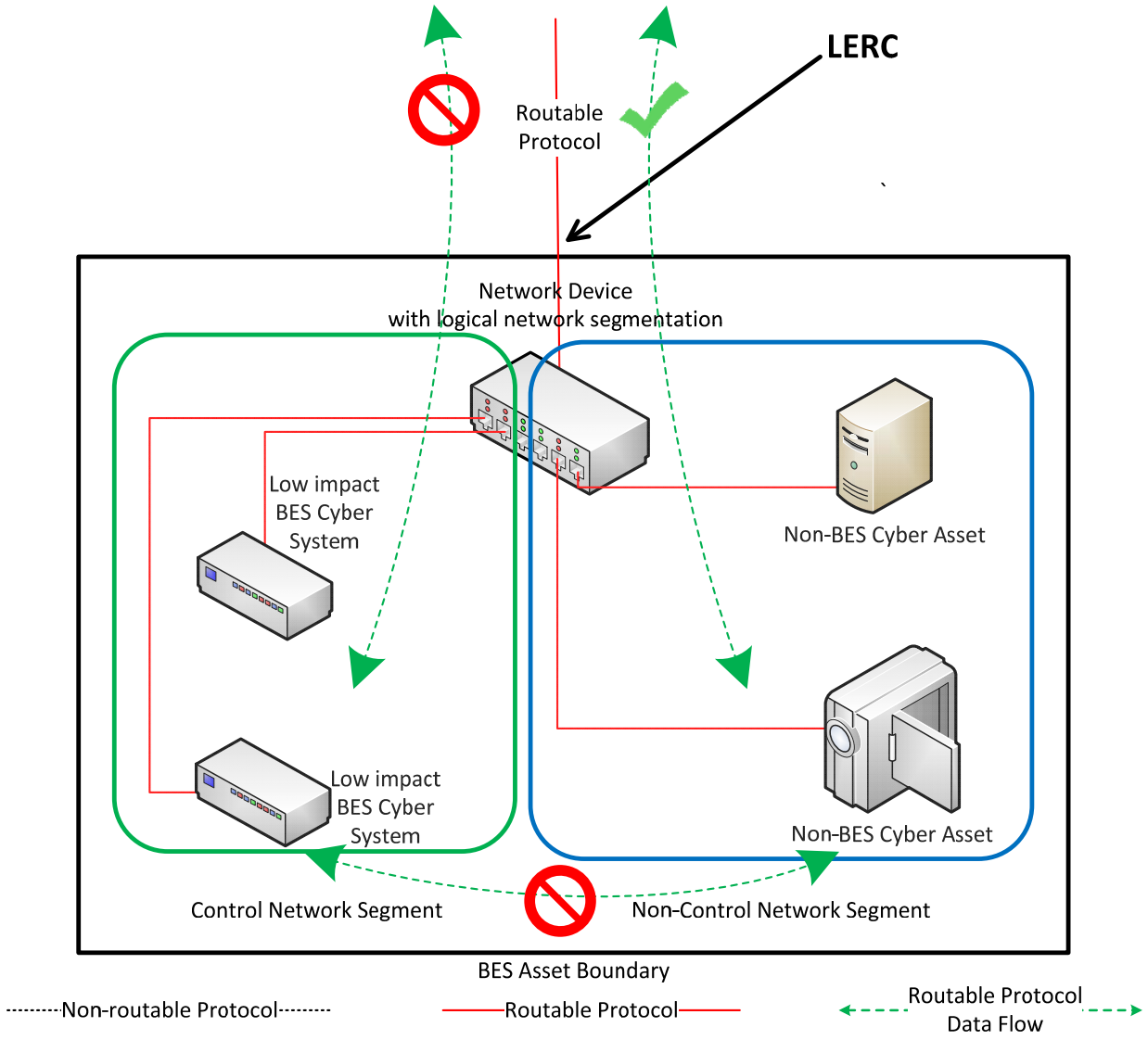
The Responsible Entity may choose to physically isolate the low impact BES Cyber System(s) from the LERC. This control is commonly referred to as an 'air gap'. The serial non-routable protocol connection and the routable protocol LERC are completely isolated from each other. There is no equipment shared with the low impact BES Cyber System(s).



Reference Model 1

LERC Reference Model 2 – Logical Isolation

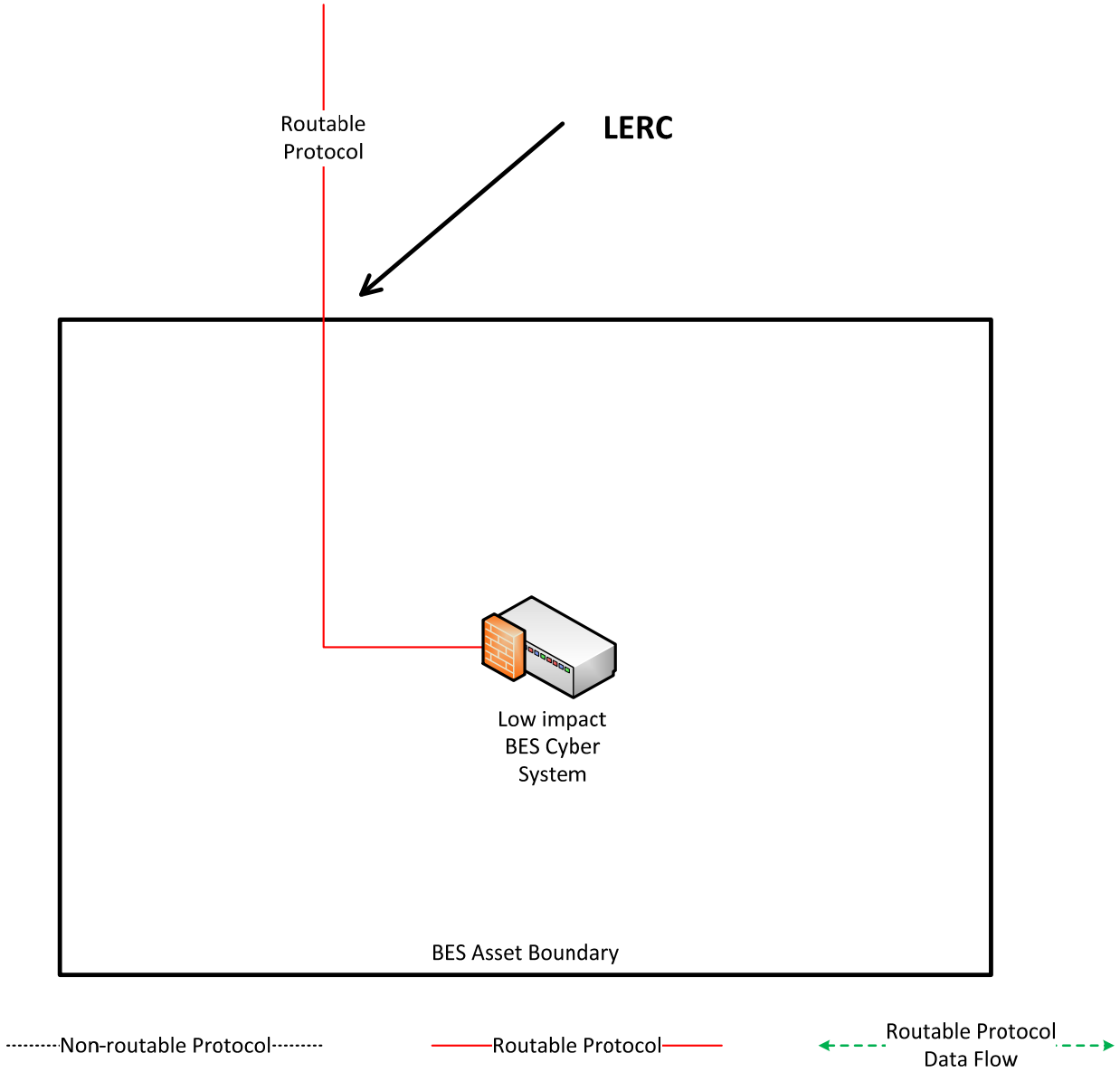
The Responsible Entity may choose to logically isolate the low impact BES Cyber System(s) from the LERC. The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s).



Reference Model 2

LERC Reference Model 3 – Host-based Inbound & Outbound Access Permissions

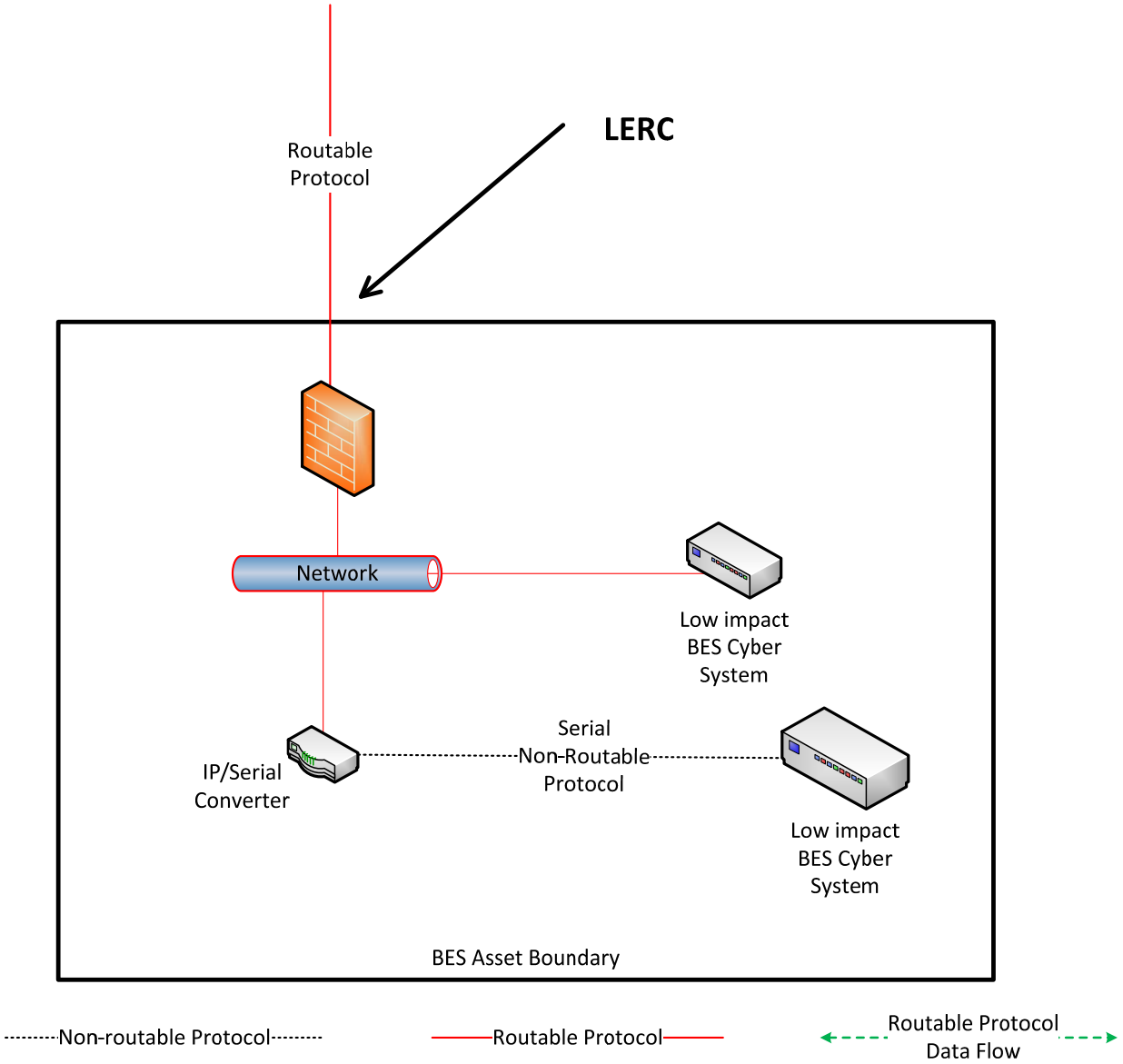
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) that manages electronic access permission so that only necessary inbound and outbound routable protocol access is allowed to the low impact BES Cyber System(s).



Reference Model 3

LERC Reference Model 4 – Network-based Inbound & Outbound Access Permissions

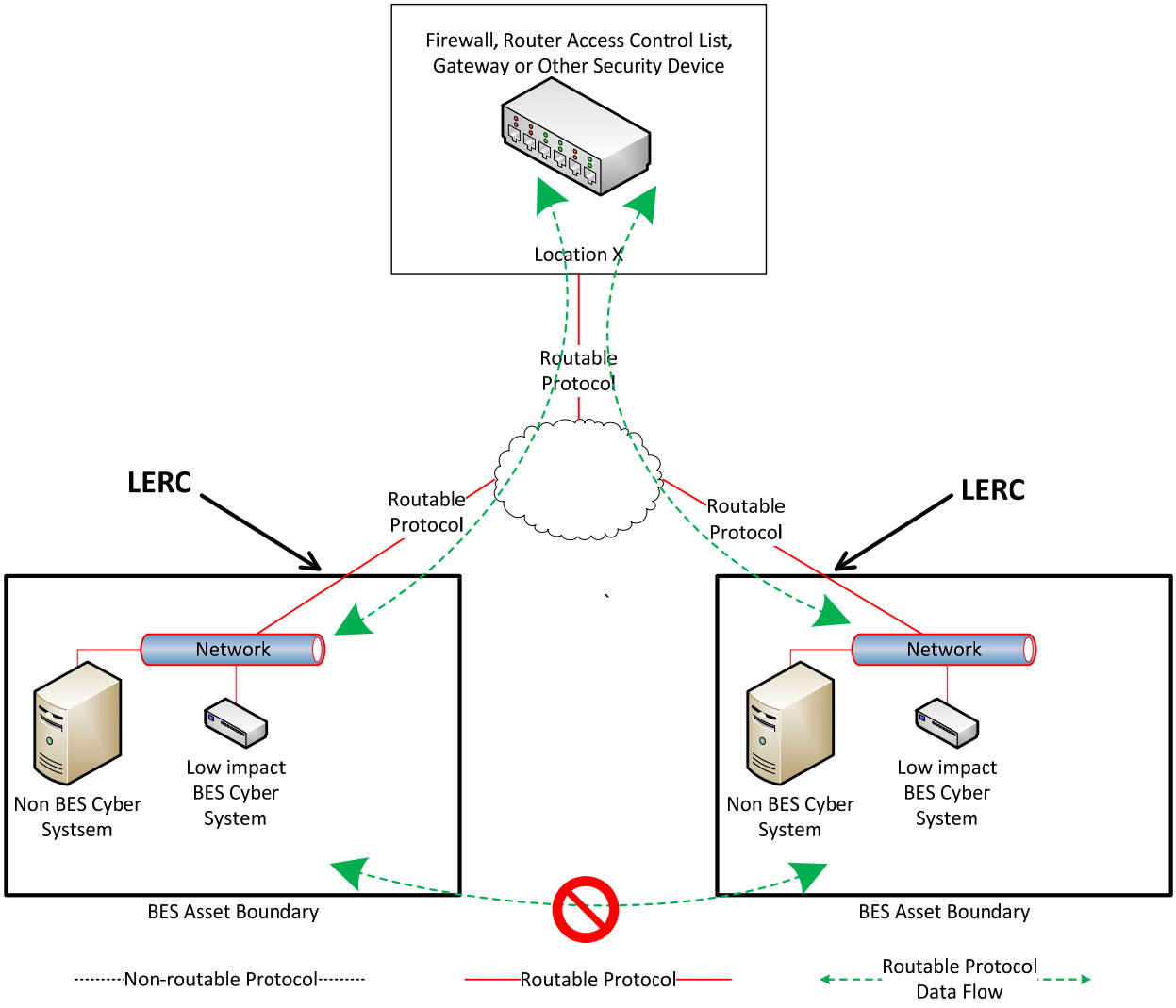
The Responsible Entity may choose to utilize a security device that permits only necessary access to the low impact BES Cyber System(s) within the BES asset. In this example, two low impact BES Cyber Systems are accessed over the LERC as the IP/Serial converter is continuing the same communications session from device(s) outside the BES asset boundary to the low impact BES Cyber Systems. The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber Systems.



Reference Model 4

LERC Reference Model 5 – Centralized Network-based Inbound & Outbound Access Permissions

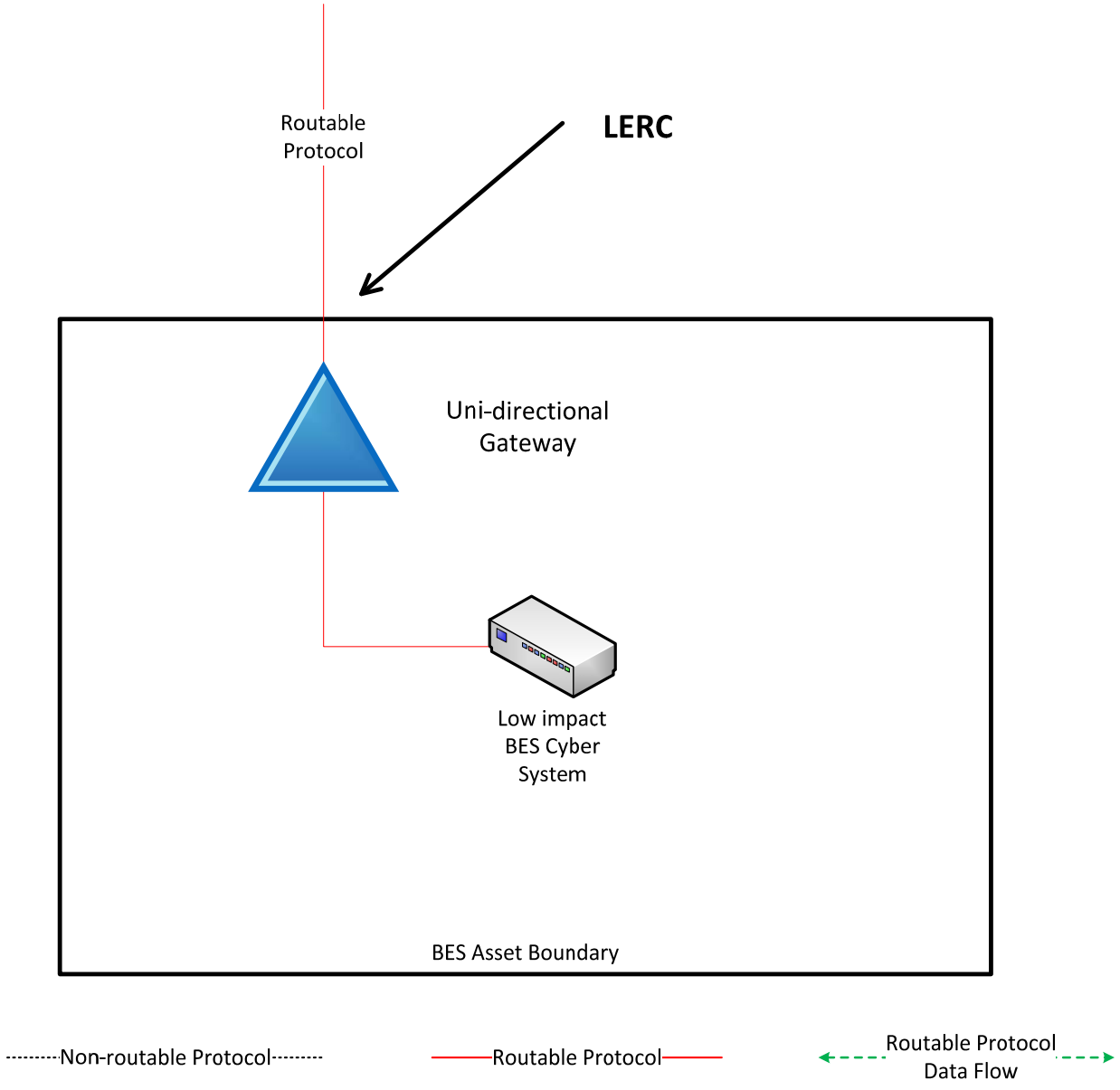
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be another BES asset. The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). Care should be taken that electronic access to or between each BES asset is through the electronic access controls at the centralized location.



Reference Model 5

LERC Reference Model 6 – Uni-directional Gateway

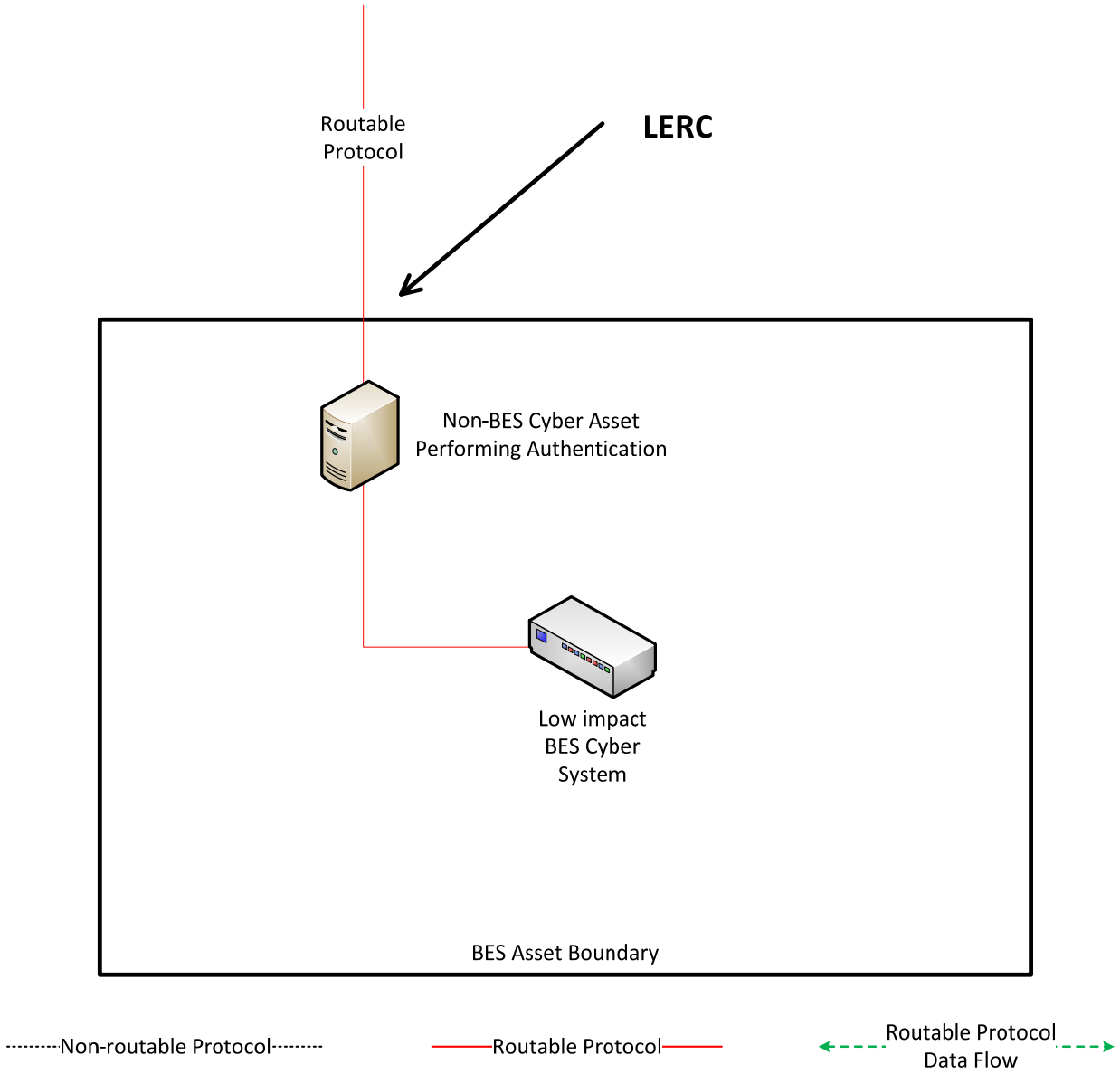
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) from the LERC due to the implementation of a "one-way" (uni-directional) path for data to flow across the BES asset boundary.



Reference Model 6

LERC Reference Model 7 – User Authentication

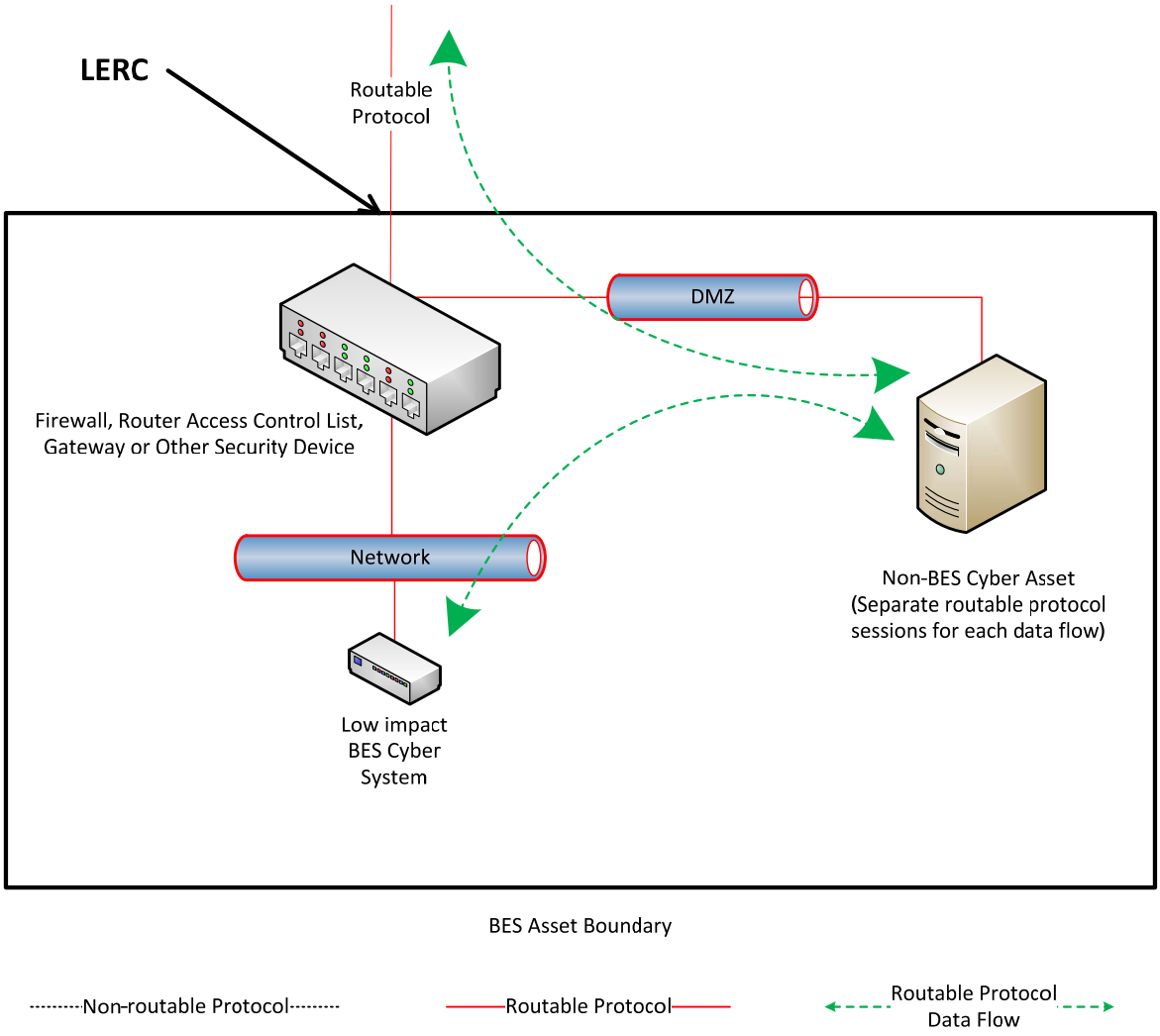
The Responsible Entity may choose to utilize a non-BES Cyber Asset between the network outside the BES asset boundary and the low impact BES Cyber System to perform user authentication for interactive access. The non-BES Cyber Asset would require authentication before establishing a new connection to the low impact BES Cyber System. The electronic access control depicted in this reference model may not meet the security objective for controlling device-to-device communication across the LERC depending on the specific system configuration in place.



Reference Model 7

LERC Reference Model 8 – Session Termination

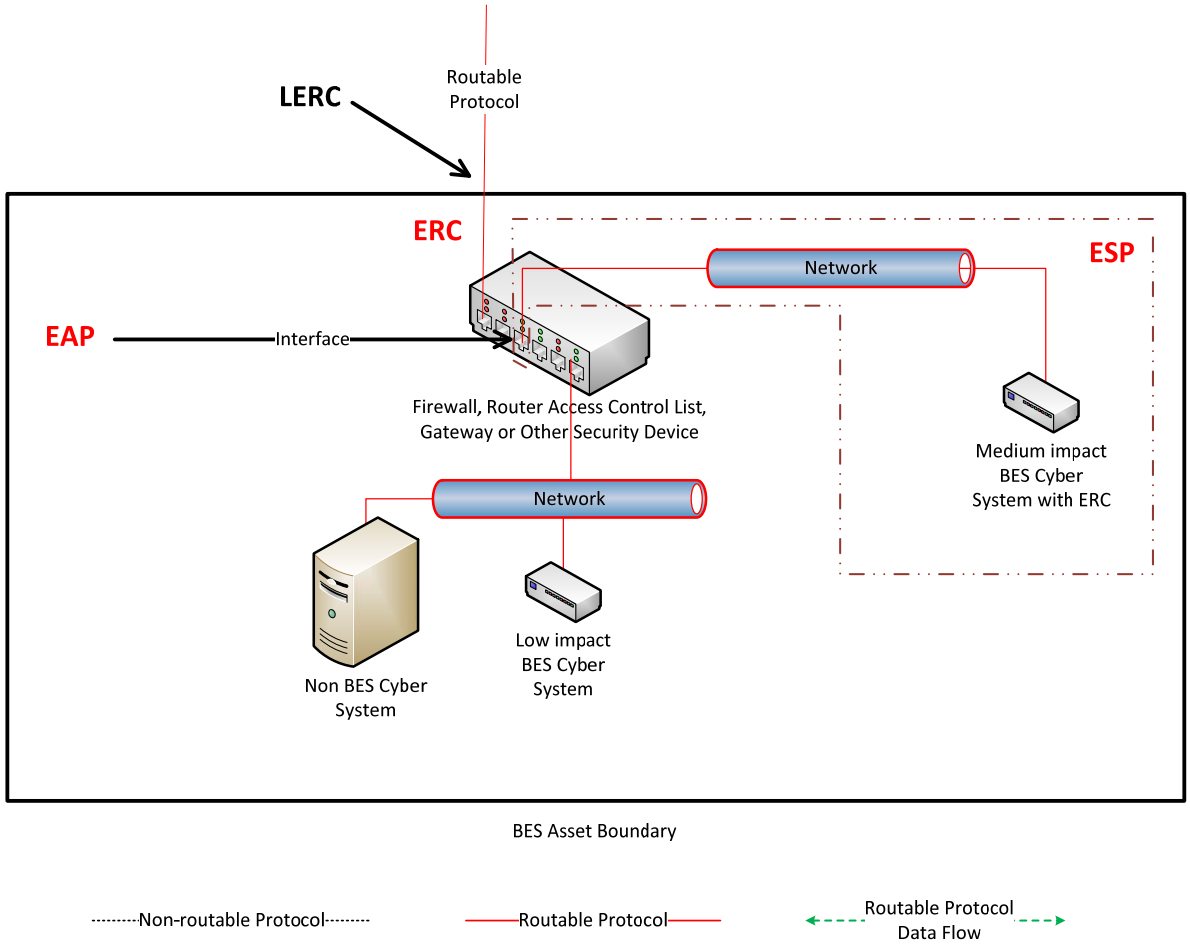
The Responsible Entity may choose to terminate routable protocol application sessions at a non-BES Cyber Asset inside the asset containing the low impact BES Cyber System(s) such that a separate application session is established to the low impact BES Cyber System(s) from the non-BES Cyber Asset (the routable session from outside the BES asset). The Responsible Entity may choose to authenticate access at a non-BES Cyber Asset either outside BES asset boundary or inside the asset containing the low impact BES Cyber System(s) such that unauthenticated access to the low impact BES Cyber System(s) is prohibited. The non-BES Cyber Asset sits on a demilitarized zone (DMZ) between the network outside the BES asset boundary and the low impact BES Cyber System(s). The non-BES Cyber Asset in the DMZ terminates the routable protocol session and establishes a new session to the low impact BES Cyber System(s). Additionally, a security device permits traffic from the network outside the BES asset boundary to flow only to and from the non-BES Cyber Asset in the DMZ (the routable session to the low impact BES Cyber System).



Reference Model 8

LERC Reference Model 9 – LERC and ERC

There is both LERC and ERC present in this reference model because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the BES asset. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) device to provide electronic access controls for the LERC. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing low impact electronic access controls.



Reference Model 9

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- An asset has LERC due to a BES Cyber System within it having a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber

Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP

Senior Manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for “clear lines of authority and ownership for security matters.” With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

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.

Description of Current Draft

This draft of CIP-003-7 is addressing the directive issued by the Federal Energy Regulatory Commission (Commission) in paragraph 73 of Order No. 822 which reads:

> [T]he Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule approving revisions to the cybersecurity Critical Infrastructure Protection (CIP) standards.

Previously, the Guidelines and Technical Basis had approximately 10 pages of explanation and numerous reference models to describe different forms of direct vs. indirect access that could be used to determine whether Low Impact External Routable Connectivity existed and thus whether a Low Impact BES Cyber System Electronic Access Point (LEAP) was required.

In this revision, the term *Low Impact External Routable Connectivity* has been changed to *Low Impact External Routable Communication (LERC*) and simplified so that it is an attribute of a BES asset concerning whether there is routable protocol communications across the asset boundary without regard to 'direct vs. indirect' access that may occur. This greatly simplifies and clarifies the definition of LERC. It removes the dependency between the electronic access controls that may be in place and having those controls determine whether LERC exists or not. For those BES assets that have LERC, the SDT changed the requirement from requiring a LEAP to requiring electronic access controls to "permit only necessary electronic access to low impact BES Cyber Systems" (revised Attachment 1, Section 3.1) within the BES asset and expanded the Guidelines and Technical Basis with numerous examples of electronic access controls.

Given the modified definition of LERC and the proposed modifications in Reliability CIP-003-7, there is no longer a need for the NERC Glossary term Low Impact BES Cyber System Electronic Access Point (LEAP). Consequently, NERC is proposing that term for retirement.

In summary, the CIP Standard Drafting Team revised CIP-003-7, Attachments 1 and 2, Sections 2 and 3 and the associated High VSL for Requirement R2. Non-substantive errata changes were also made within the standard, including changing "ES-ISAC" to "E-ISAC".

Completed Actions	Date
Standard Authorization Request (SAR) approved	July 20, 2016
Draft 1 of CIP-003-7 posted for formal comment and initial ballot	July 21 – September 6, 2016

Anticipated Actions	Date
10-day final ballot	October, 2016
NERC Board of Trustees (BOT) adoption	November, 2016

A. Introduction

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

2. **Number:** CIP-003-~~6~~7

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 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 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 SPS or RAS where the SPS or 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-~~6:~~ 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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3 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.

4.2.3.4 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-~~6~~7.

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single

cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls for Low Impact External Routable ~~Connectivity~~Communication (LERC) and Dial-up Connectivity; and

1.2.4. Cyber Security Incident response

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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented one or more incident response plans	The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of	The Responsible Entity failed to document or implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to ~~CIP-003-6,~~ Requirement R2, Attachment 1. (R2~~)~~).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, but failed to document one or more Cyber Security Incident response plans according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to ~~CIP-003-6,~~ Requirement R2,	within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. ~~(R2)~~ (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~E-ISAC) according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented ~~and implemented electronic access controls for LERC, but failed to implement a LEAP or permit inbound and outbound access according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)~~ ~~OR~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 4. (R2)	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~E-ISAC) according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to ~~CIP-003-6,~~	~~The Responsible Entity documented and implemented~~ electronic access controls for its assets containing low impact BES Cyber Systems, but failed to ~~document and~~ implement ~~authentication of all Dial-up Connectivity, if any, that provides~~the electronic access ~~to low impact BES Cyber Systems~~controls according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 3. (R2)	security controls according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 2. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			document this change in less than 40 calendar days of the change. (R3)	days but did document this change in less than 50 calendar days of the change. (R3)	less than 60 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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

Version	Date	Action	Change Tracking
			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 devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees.	Revised to address FERC Order 822 directive regarding definition of LERC

~~CIP-003-6 –~~ Attachment 1

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

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

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

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

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

Section 3. Electronic Access Controls: Each Responsible Entity shall:

3.1 ~~For~~Implement electronic access control(s) for LERC, if any, ~~implement a LEAP~~ to permit only necessary ~~inbound and outbound bi-directional routable protocol access; and~~electronic access to low impact BES Cyber System(s).

3.2 Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~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.

~~CIP-003-6 –~~ Attachment 2

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

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

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

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

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

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

1. Documentation, such as representative diagrams or lists of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; authenticating users; air-gapping networks; terminating routable protocol sessions on a non-BES Cyber Asset; implementing unidirectional gateways) showing that ~~inbound and outbound connections~~ for ~~any LEAP(s) are~~LERC at each asset or group of assets containing low impact BES Cyber Systems, is confined ~~to~~ only ~~those~~to that access the Responsible Entity deems necessary ~~(e.g., by restricting IP addresses, ports, or services); and documentation~~; and

~~1.~~2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~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.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-~~6~~7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-~~6~~7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any *assets containing low impact BES Cyber Systems*~~,~~, also referred to herein as ~~("~~BES assets~~"),~~ the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-~~6~~7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in

NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts

- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

Using the list of assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that addresses objective criteria for the protection of low impact BES Cyber Systems. The protections required by Requirement R2 reflect the level of risk that misuse or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the required protections are part of a program that covers the low impact BES Cyber Systems

collectively either at an asset or site level (assets containing low impact BES Cyber Systems), but not at an individual device or system level.

There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and Dial-up Connectivity, and (4) Cyber Security Incident response.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. Guidance for each of the four subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The Responsible Entity is not required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or “If you see something, say something” campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems ~~at assets containing low impact BES~~ within the asset, and (2) Cyber ~~System~~Assets that implement the electronic access control(s) ~~and (2) LEAPs~~specified by the Responsible Entity in Section 3, if any. If ~~the LEAP is~~these Cyber Assets are located within the BES asset and ~~inherits~~inherit the same controls outlined in Section 2, this can be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility in the selection of the methods used to meet the objective to control physical access to the asset(s) containing low impact BES Cyber ~~Systems,~~System(s) or the low impact BES Cyber Systems themselves, ~~or LEAPs~~as well as physical protection of the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. User authorization programs and lists of

authorized users for physical access are not required although they are an option to meet the security objective.

The objective is to control the physical access based on need as determined by the Responsible Entity. The need can be documented at the policy level for access to the site or systems, including LEAPs.. The requirement does not obligate an entity to specify a need for each access or authorization of a user for access.

Monitoring as a physical security control can be used as a complement or an alternative to access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of boundary protectionselectronic access controls for *assets containing low impact BES Cyber Systems*, also referred to herein as ("BES assets") when the low impact BES Cyber Systems have bi-directional external routable protocol communication (LERC) or Dial-up Connectivity is present to devices external toor from the asset containing the low impact BES Cyber Systems.System(s). The establishment of boundary protectionselectronic access controls is intended to control communication either into the asset containing low impact BES Cyber System(s) or to the low impact BES Cyber System itself to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. The term "electronic access control" is used in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing. The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or In the case where there is no LERC or Dial-up Connectivity present. In the case where there is no external bi-directional routable protocol communication, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the controls that meet their operational needs while meeting the security objective of allowing only necessary electronic access to low impact BES Cyber Systems.

In essence, Responsible Entities are to determine LERC or Dial-up Connectivity for their BES assets and then, if present, document and implement electronic access control(s).

Determining LERC

The defined terms LERC and LEAP are term Low Impact External Routable Communication (LERC) is used to avoid confusion with the similar terms term External Routable Connectivity (ERC) used for high and medium impact BES Cyber Systems (e.g., External Routable Connectivity (ERC) or as these terms are different concepts. The input to this requirement from CIP-002 is a list of assets containing low impact BES Cyber Systems, therefore LERC is an attribute of a BES asset and involves routable protocol communications to or from the BES asset (crossing the

asset boundary) without regard to connectivity to Cyber Assets within the BES asset. ERC on the other hand is an attribute of an individual high or medium impact BES Cyber System and is relative to an Electronic ~~Access Point (EAP)). To future-proof the standards, and in~~Security Perimeter (ESP).

With LERC being a BES asset level attribute, it is used as a higher level filter to exclude from further consideration those assets containing low impact BES Cyber Systems that have no routable protocol communications to them from outside the BES asset. Responsible Entities can then concentrate their electronic access control efforts on those BES assets that do have LERC. However, this also means that LERC can exist for a BES asset even if there is no routable protocol connectivity to any low impact BES Cyber System within the BES asset.

In order to avoid future technology issues, the ~~definitions~~LERC definition specifically ~~exclude "point-to-point~~excludes communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between ~~Transmission station or substation~~non-Control Center BES assets containing low impact BES Cyber Systems~~,"~~, such as IEC 61850 messaging. This does not exclude Control Center to field communication but rather excludes the communication between the intelligent electronic devices ~~themselves.~~(e.g. relays) in the field. A Responsible Entity using this technology is not expected to implement ~~a LEAP~~the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive requirements related to this technology nor to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Determining Asset Boundary

As LERC is a BES asset level attribute, it involves a determination by the Responsible Entity of a BES asset boundary for their assets containing low impact BES Cyber Systems. This boundary will vary by BES asset type (Control Center, substation, generation resource) and the specific configuration of the BES asset. The intent is for the Responsible Entity to define the BES asset boundary such that the low impact BES Cyber System(s) that are located at the BES asset are contained within the BES asset boundary. This is strictly for determining what constitutes the BES "asset" and for determining which routable protocol communications and networks are *internal* or *inside* or *local* to the BES asset and which are *external to or outside* the BES asset. This is not an Electronic Security Perimeter or Physical Security Perimeter as defined for medium and high impact BES Cyber Systems. For the asset containing low impact BES Cyber System(s), the BES asset boundary is synonymous to the concept of a "logical border" demarcation where routable protocol communication (e.g. LERC) enters and exits the BES asset containing the low impact BES Cyber System. Some examples of ways a Responsible Entity may determine BES asset boundaries are:

- For Control Centers
  - Designated areas (room(s) or floor(s)) if the Control Center is located within a larger building.
  - A building if in a dedicated building on a shared campus.

- The property/fence line if the Control Center is a dedicated facility on dedicated property.

- For substations, this could be the property/fence line or the control house.
- For generation resources:
  - Fossil/hydro generating facilities: This could be the property/fence line. If pumps or wells or other equipment that are part of the plant asset are outside the property line, then the BES asset boundary could expand to accommodate all that is considered part of the plant.
  - Solar farms: This could be the property line(s) or fence(s) surrounding all solar panels and interconnection facilities.
  - Wind farms: This could be the collection of individual turbines plus the equipment needed for interconnection.
  - Cogeneration facilities: This could be the identified portion of the larger plant that performs generation.

Determining Electronic Access Controls

Once a Responsible Entity has determined that LERC exists at the BES asset boundary, the Responsible Entity documents and implements its chosen electronic access control(s). The control(s) must allow only "necessary" access as determined by the Responsible Entity and they need to be able to explain the reasons for the electronic access permitted with their electronic access controls. The reasoning for the "necessary" access controls can be documented within the Responsible Entity's cyber security plan(s) or other policies or procedures associated with the electronic access controls.

Concept Diagrams

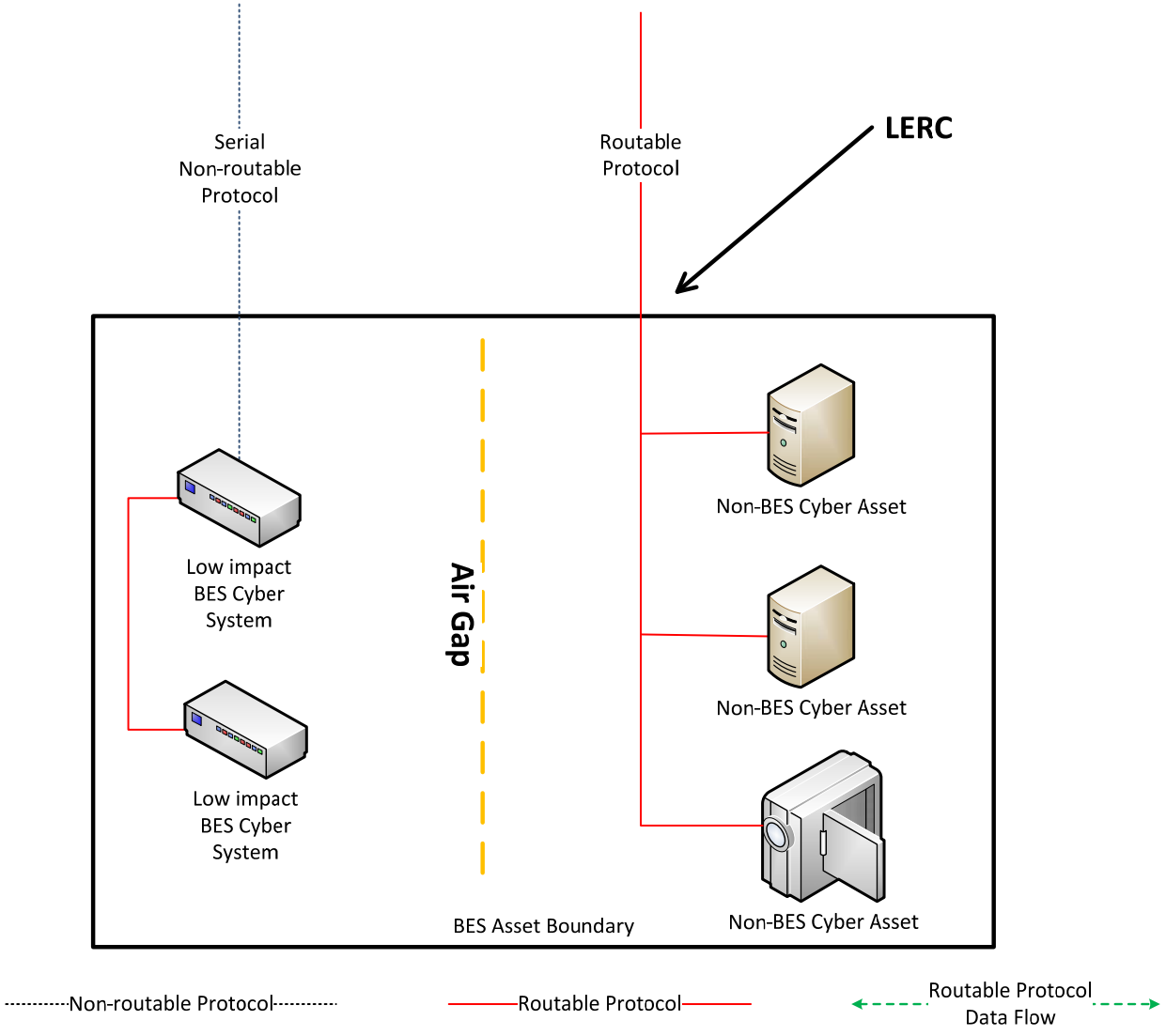
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the security objective of permitting only necessary access to low impact BES Cyber Systems must be met when there is LERC to a BES asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- LERC is present in each diagram.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.
- The term "BES Asset Boundary" is capitalized in the diagrams but it is not a defined term.

LERC Reference Model 1 – Physical Isolation

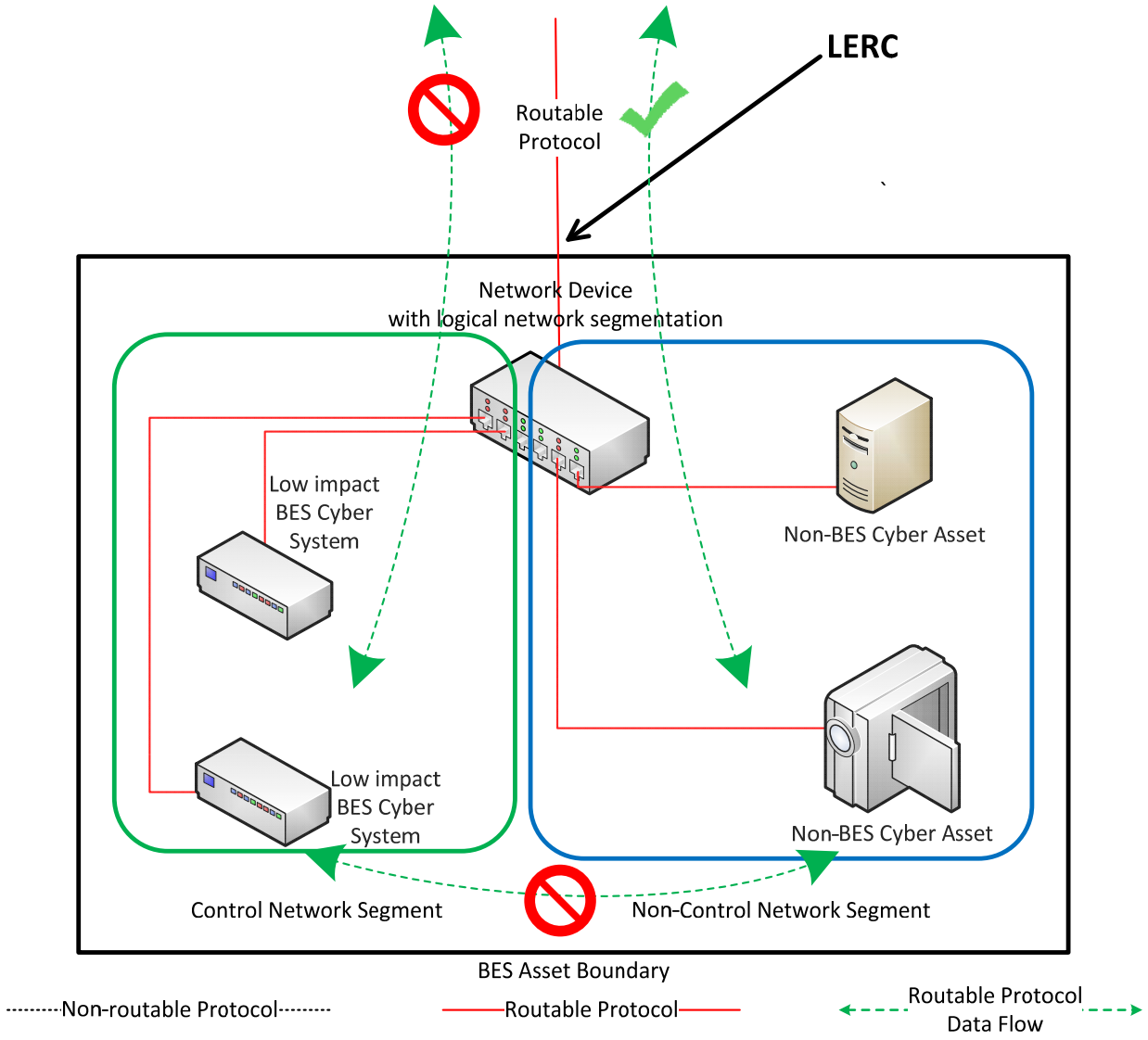
The Responsible Entity may choose to physically isolate the low impact BES Cyber System(s) from the LERC. This control is commonly referred to as an 'air gap'. The serial non-routable protocol connection and the routable protocol LERC are completely isolated from each other. There is no equipment shared with the low impact BES Cyber System(s).



Reference Model 1

LERC Reference Model 2 – Logical Isolation

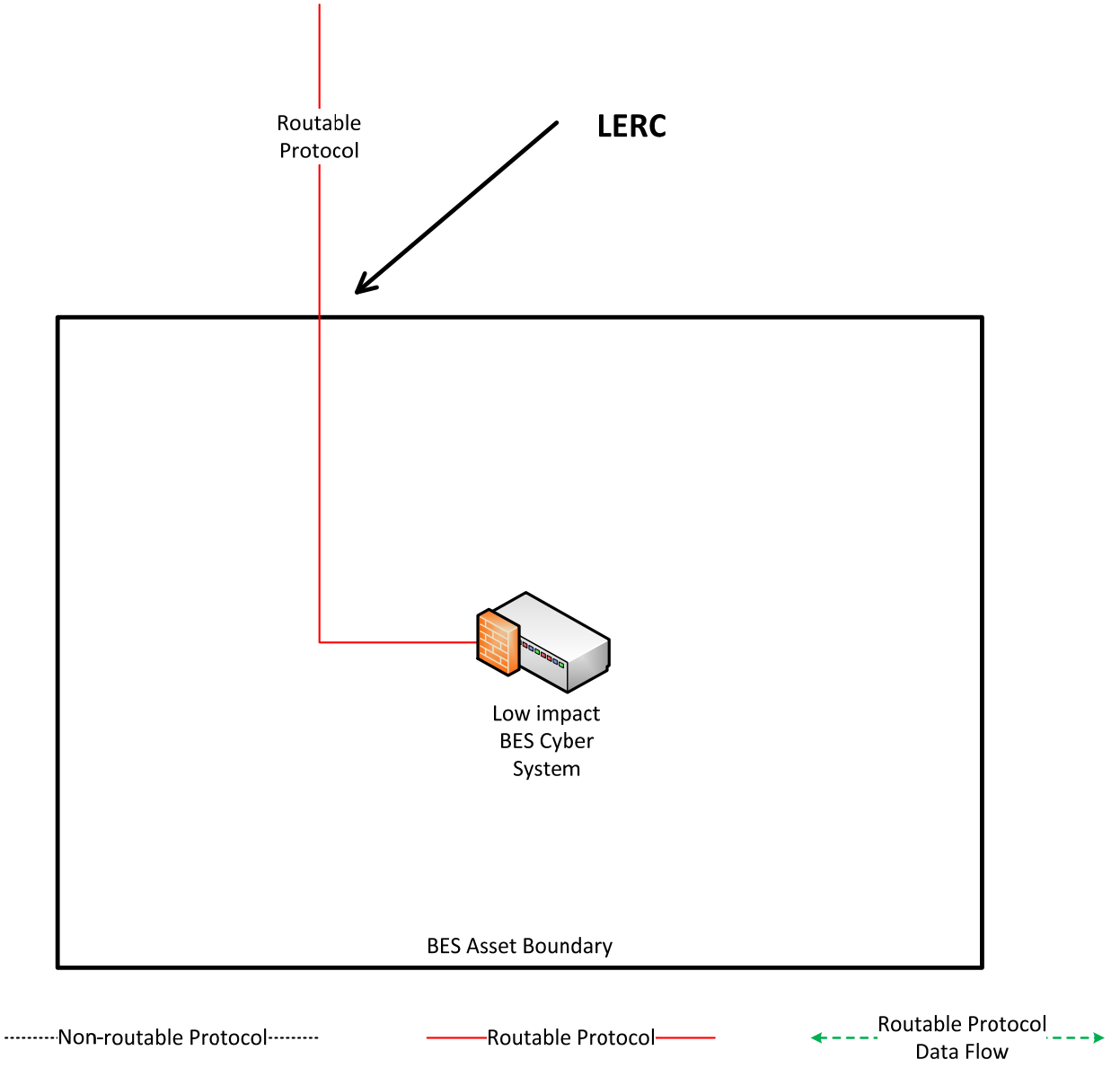
The Responsible Entity may choose to logically isolate the low impact BES Cyber System(s) from the LERC. The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s).



Reference Model 2

LERC Reference Model 3 – Host-based Inbound & Outbound Access Permissions

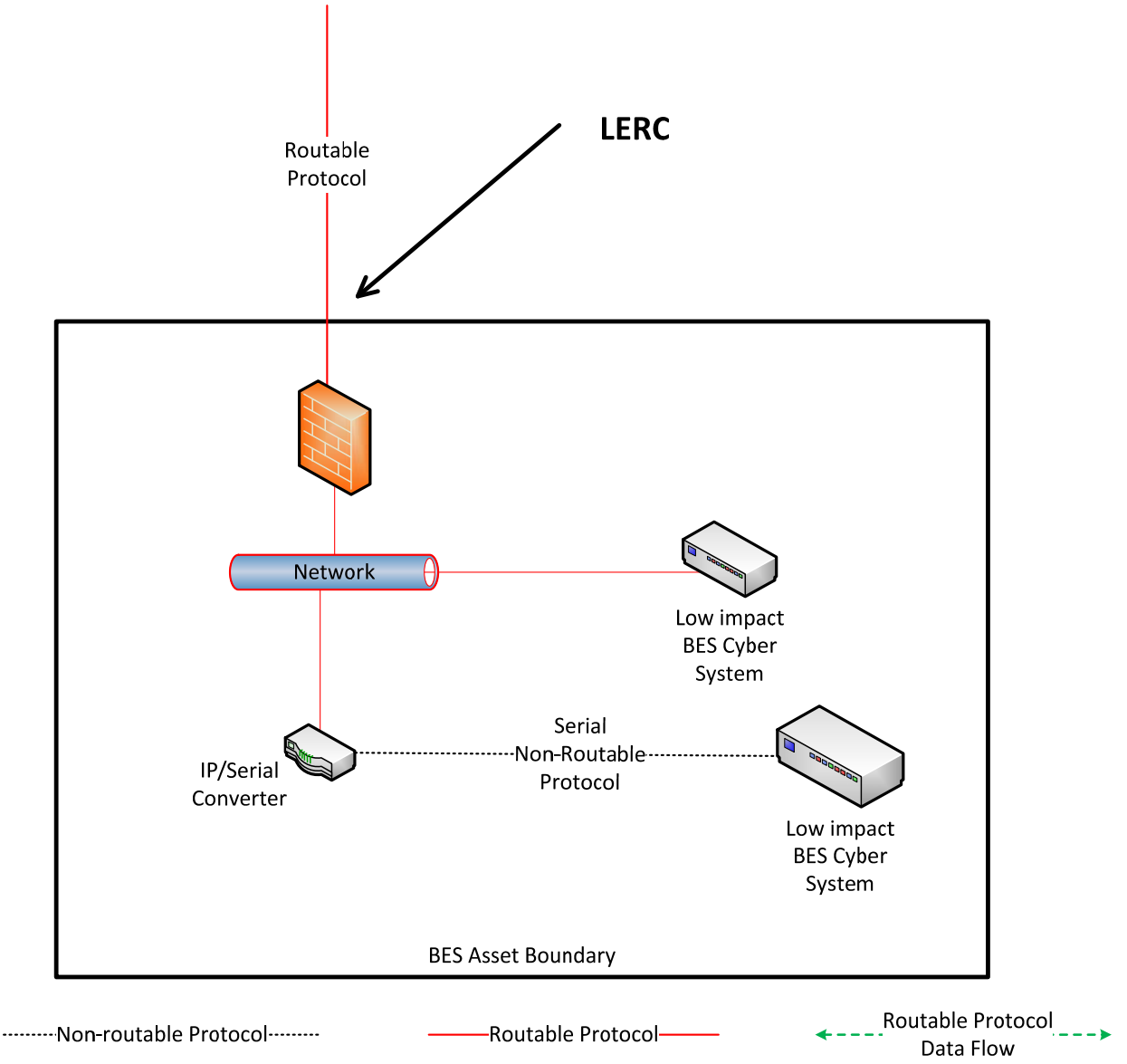
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) that manages electronic access permission so that only necessary inbound and outbound routable protocol access is allowed to the low impact BES Cyber System(s).



Reference Model 3

LERC Reference Model 4 – Network-based Inbound & Outbound Access Permissions

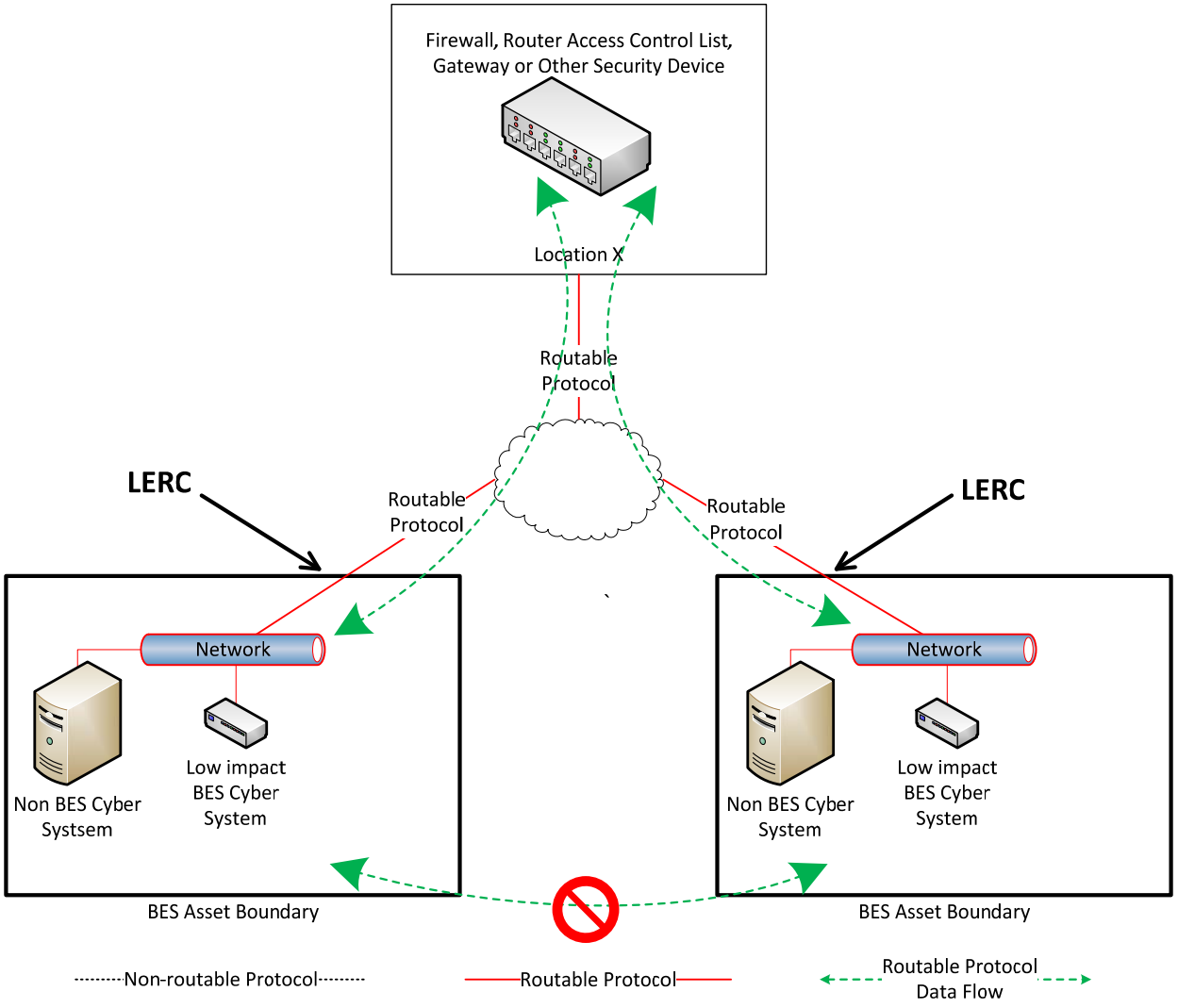
The Responsible Entity may choose to utilize a security device that permits only necessary access to the low impact BES Cyber System(s) within the BES asset. In this example, two low impact BES Cyber Systems are accessed over the LERC as the IP/Serial converter is continuing the same communications session from device(s) outside the BES asset boundary to the low impact BES Cyber Systems. The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber Systems.



Reference Model 4

LERC Reference Model 5 – Centralized Network-based Inbound & Outbound Access Permissions

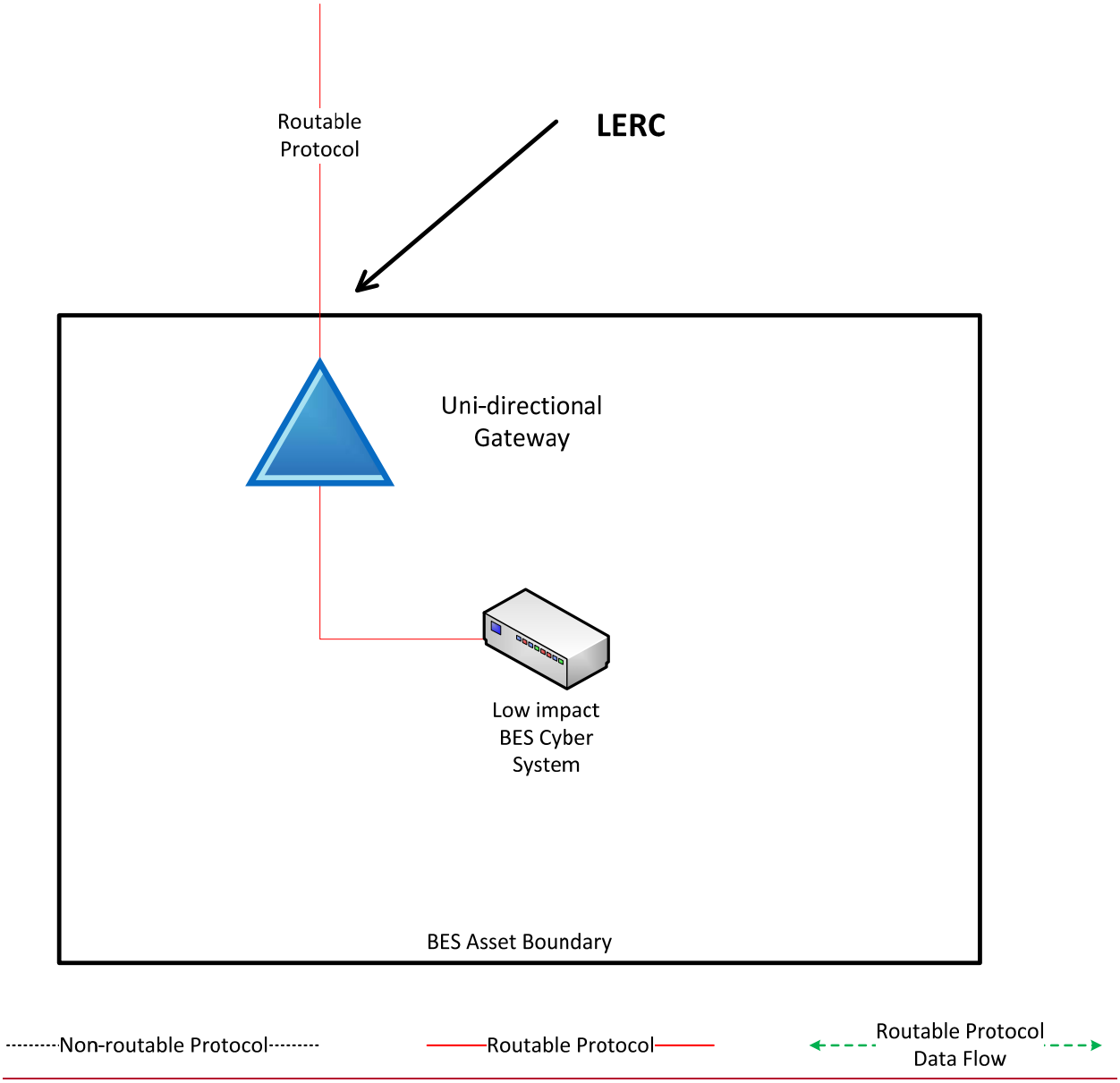
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be another BES asset. The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). Care should be taken that electronic access to or between each BES asset is through the electronic access controls at the centralized location.



Reference Model 5

LERC Reference Model 6 – Uni-directional Gateway

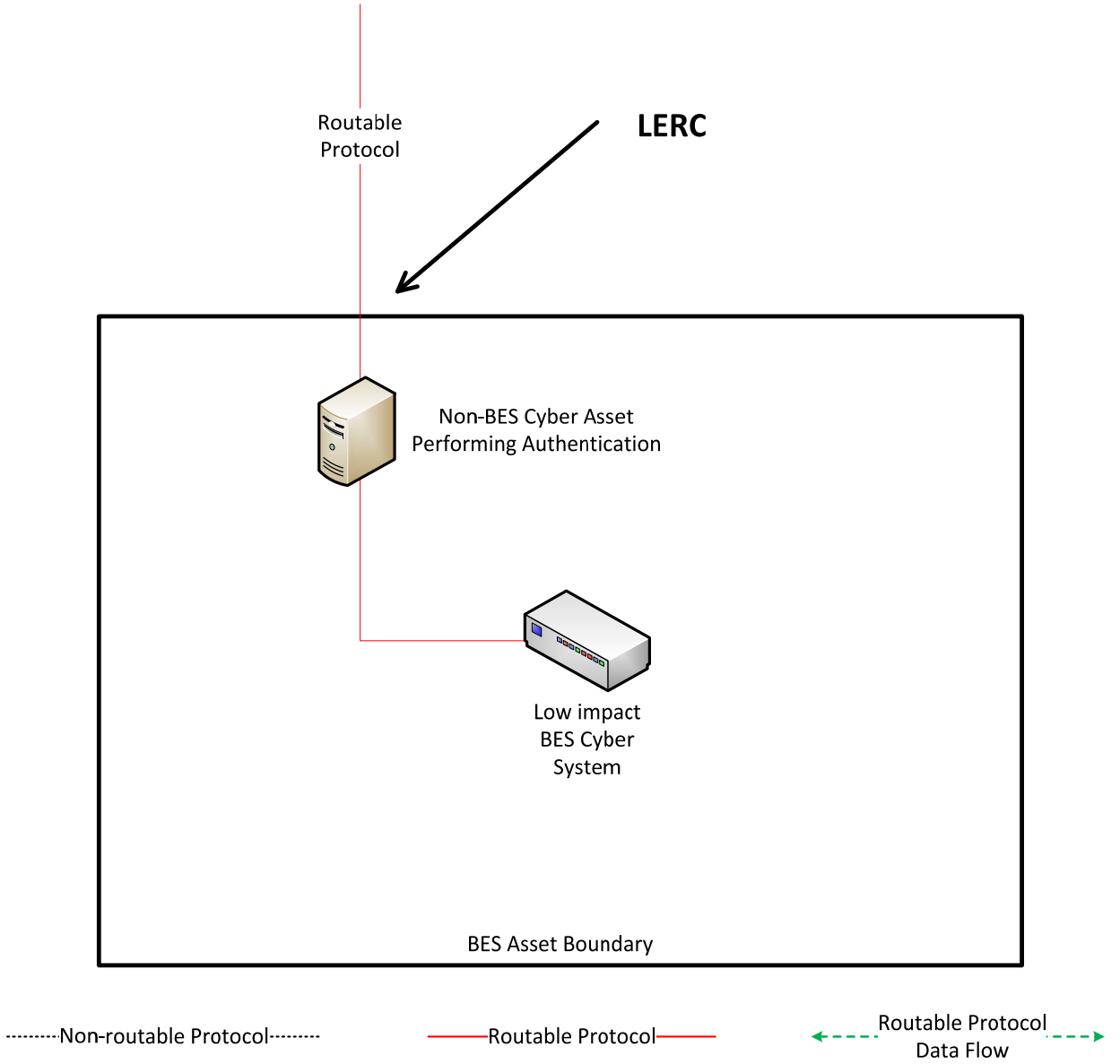
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) from the LERC due to the implementation of a "one-way" (uni-directional) path for data to flow across the BES asset boundary.



Reference Model 6

LERC Reference Model 7 – User Authentication

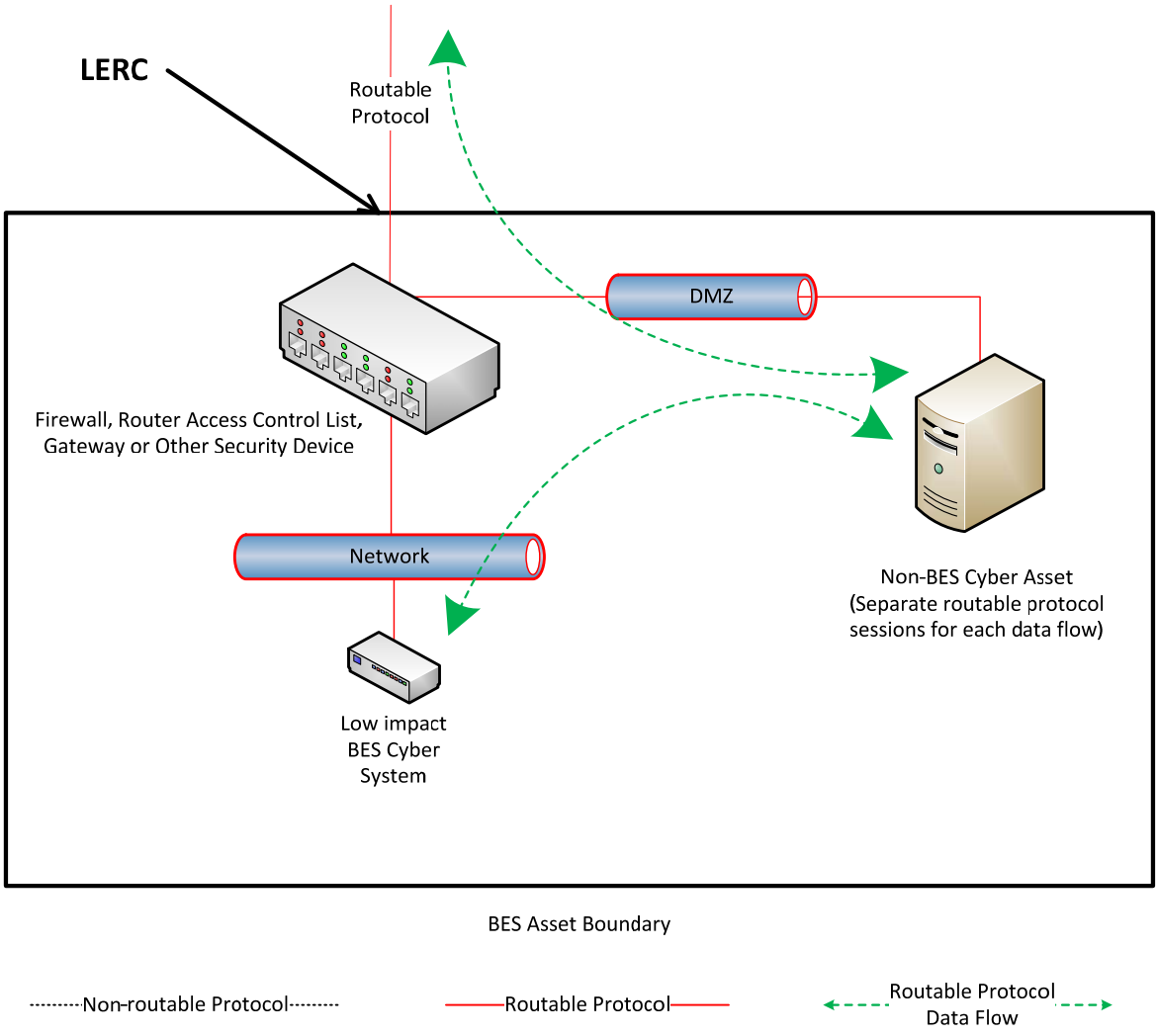
The Responsible Entity may choose to utilize a non-BES Cyber Asset between the network outside the BES asset boundary and the low impact BES Cyber System to perform user authentication for interactive access. The non-BES Cyber Asset would require authentication before establishing a new connection to the low impact BES Cyber System. The electronic access control depicted in this reference model may not meet the security objective for controlling device-to-device communication across the LERC depending on the specific system configuration in place.



Reference Model 7

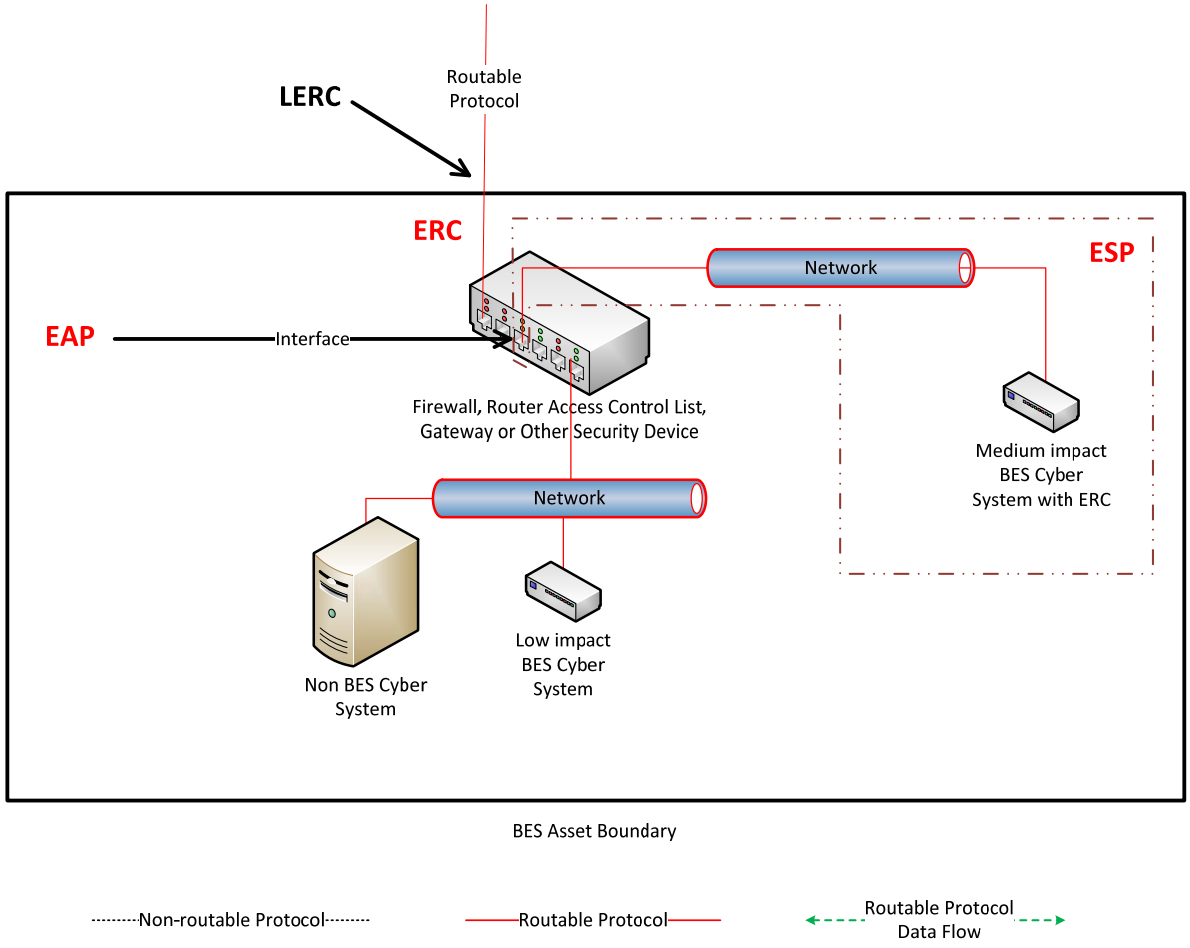
LERC Reference Model 8 – Session Termination

The Responsible Entity may choose to terminate routable protocol application sessions at a non-BES Cyber Asset inside the asset containing the low impact BES Cyber System(s) such that a separate application session is established to the low impact BES Cyber System(s) from the non-BES Cyber Asset (the routable session from outside the BES asset). The Responsible Entity may choose to authenticate access at a non-BES Cyber Asset either outside BES asset boundary or inside the asset containing the low impact BES Cyber System(s) such that unauthenticated access to the low impact BES Cyber System(s) is prohibited. The non-BES Cyber Asset sits on a demilitarized zone (DMZ) between the network outside the BES asset boundary and the low impact BES Cyber System(s). The non-BES Cyber Asset in the DMZ terminates the routable protocol session and establishes a new session to the low impact BES Cyber System(s). Additionally, a security device permits traffic from the network outside the BES asset boundary to flow only to and from the non-BES Cyber Asset in the DMZ (the routable session to the low impact BES Cyber System).



LERC Reference Model 9 – LERC and ERC

There is both LERC and ERC present in this reference model because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the BES asset. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) device to provide electronic access controls for the LERC. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing low impact electronic access controls.



Reference Model 9

When determining whether there is LERC to the low impact BES Cyber System, the definition uses the phrases "direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection." The intent of "direct" in the definition is to indicate LERC exists if a person is sitting at another device outside of the asset containing the low impact BES Cyber System, and the person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session even if there is a serial-to-routable protocol conversion. The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for "device-to-device connection," LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication to or from the low impact BES Cyber System.

When identifying a LEAP, Responsible Entities are provided flexibility in the selection of the interface on a Cyber Asset that controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, the internal interface on a router that has implemented an access control list (ACL), or other security device. The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required to reside at the asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP per asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber Systems. Locating the Cyber Asset with multiple LEAPs at an external location with multiple assets containing low impact BES Cyber Systems "behind" it, however, should not allow uncontrolled access to assets containing low impact BES Cyber Systems sharing a Cyber Asset containing the LEAP(s).

In Reference Model 4, the communication flows through an IP/Serial converter. LERC is correctly identified in this Reference Model because the IP/Serial converter in this instance is doing nothing more than extending the communication between the low impact BES Cyber System and the Cyber Asset outside the asset containing the low impact BES Cyber System. In contrast, Reference Model 6 has placed a Cyber Asset that performs a complete break or interruption that does not allow the user or device data flow to directly communicate with the low impact BES Cyber System. The Cyber Asset in Reference Model 6 is preventing extending access to the low impact BES Cyber System from the Cyber Asset outside the asset containing the low impact BES Cyber System. The intent is that if the IP/Serial converter that is deployed only does a "pass-through" of the data flow communication, then that "pass-through" data flow communication is LERC and a LEAP is required. However, if that IP/Serial converter performs some type of authentication in the data flow at the asset containing the low impact BES Cyber System before the communication can be sent to the low impact BES Cyber System, then that type of IP/Serial converter implementation is not LERC.

~~A Cyber Asset that contains interface(s) that only perform the function of a LEAP does not meet the definition of Electronic Access Control or Monitoring System (EACMS) associated with medium or high impact BES Cyber Systems and is not subject to the requirements applicable to an EACMS. However, a Cyber Asset may contain some interfaces that function as a LEAP and other interfaces that function as an EAP for high or medium impact BES Cyber Systems. In this case, the Cyber Asset would also be subject to the requirements applicable to the EACMS associated with the medium or high impact BES Cyber Systems.~~

~~Examples of sufficient access controls may include:~~

- ~~Any LERC for the asset passes through a LEAP with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g., IP addresses, ports, or services).~~
- ~~As shown in Reference Model 1 below, the low impact BES Cyber System has a host-based firewall that is controlling the inbound and outbound access. In this model, it is also possible that the host-based firewall could be on a non-BES Cyber Asset. The intent is that the host-based firewall controls the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in the business network.~~
- ~~As shown in Reference Model 5 below, a non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that the non-BES Cyber Asset has provided a "protocol break" so that access to the low impact BES Cyber System is only from the non-BES Cyber Asset that is located within the asset containing the low impact BES Cyber System.~~

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

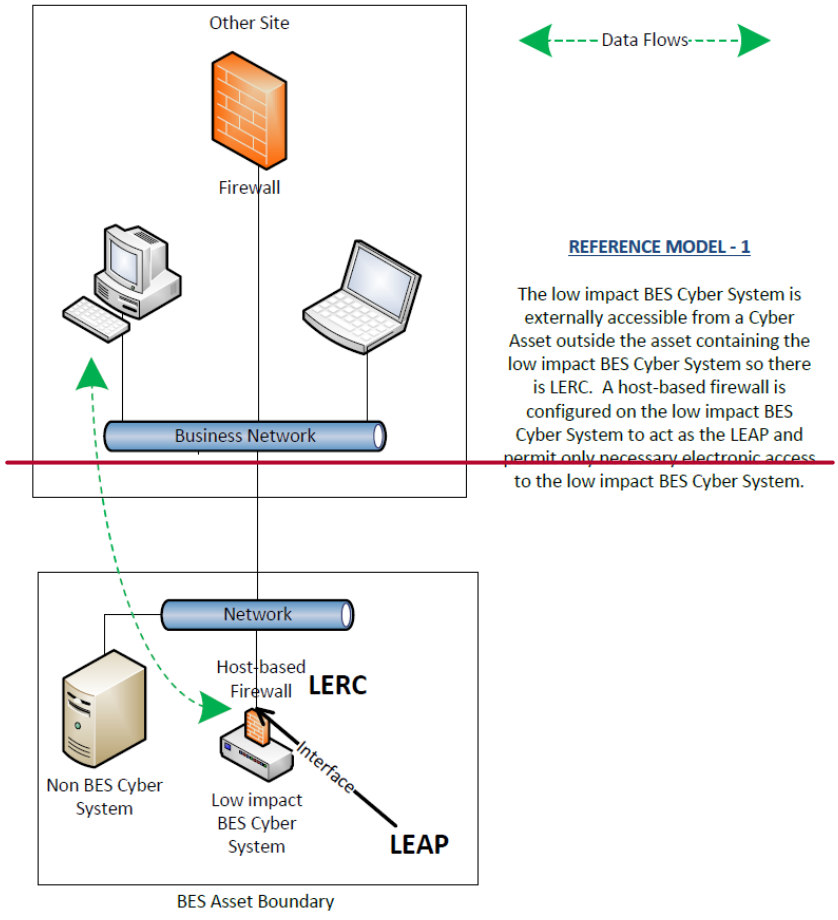
Insufficient Access Controls

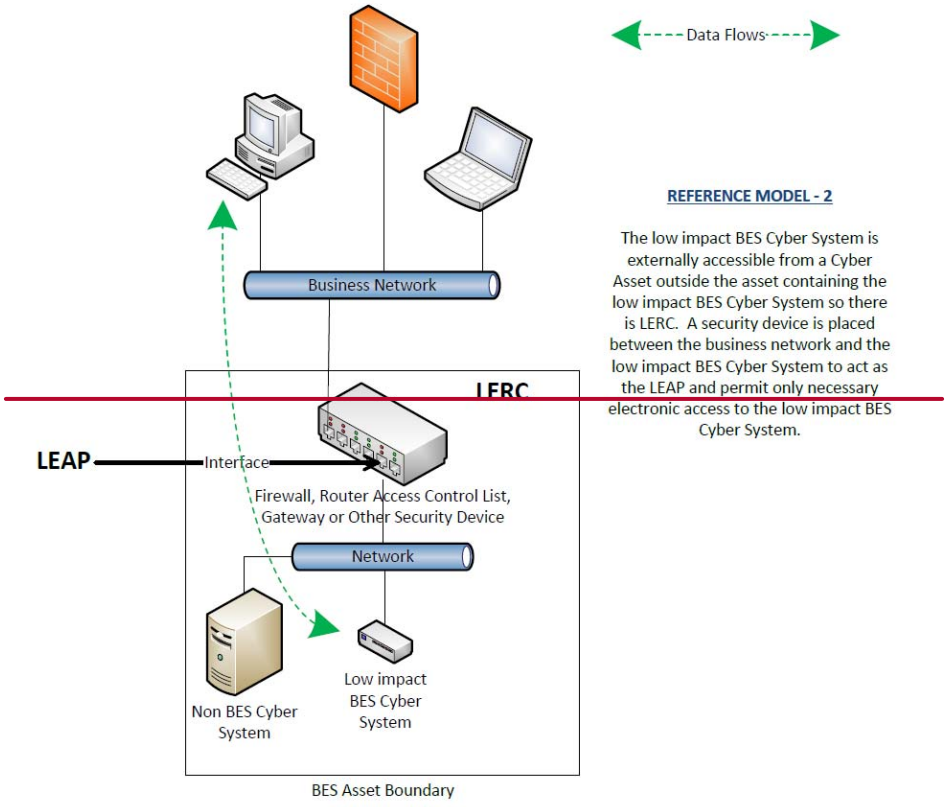
Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

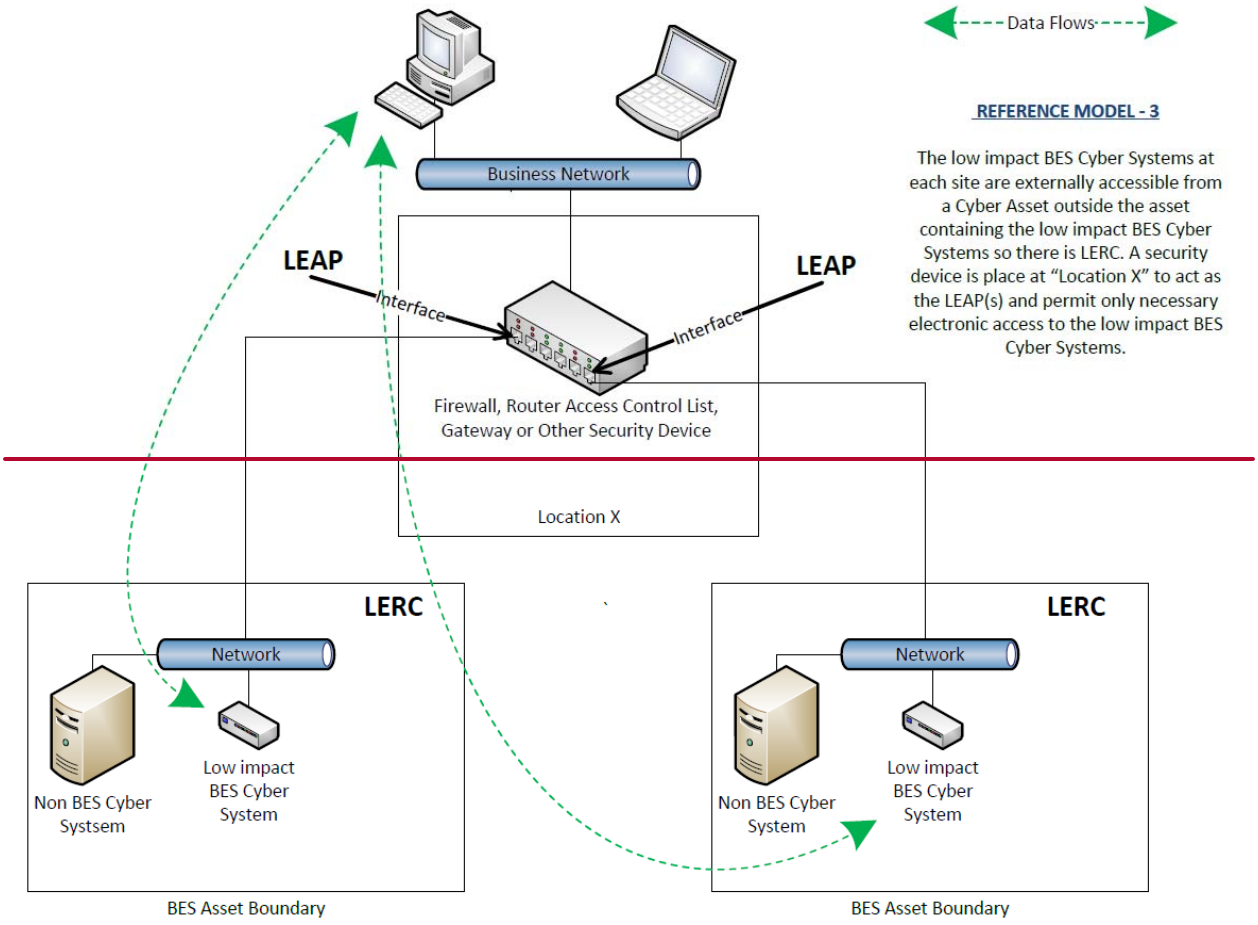
- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- An asset has LERC due to a BES Cyber System within it having a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- ~~In Reference Model 5, using just dual~~Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide

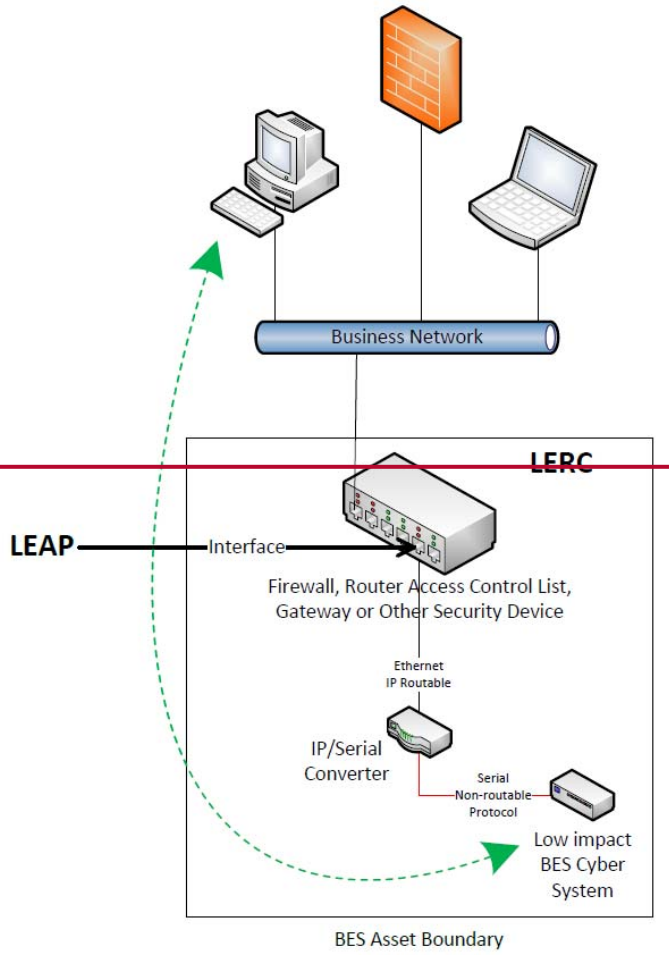
separation between the low impact BES Cyber System(s) and the ~~business~~external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security ~~device~~devices on ~~that~~the non-BES Cyber Asset.

~~The following diagrams provide reference examples intended to illustrate how to determine whether there is LERC and for implementing a LEAP. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.~~




Data Flows
REFERENCE MODEL - 2
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.
Business Network
LERC
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

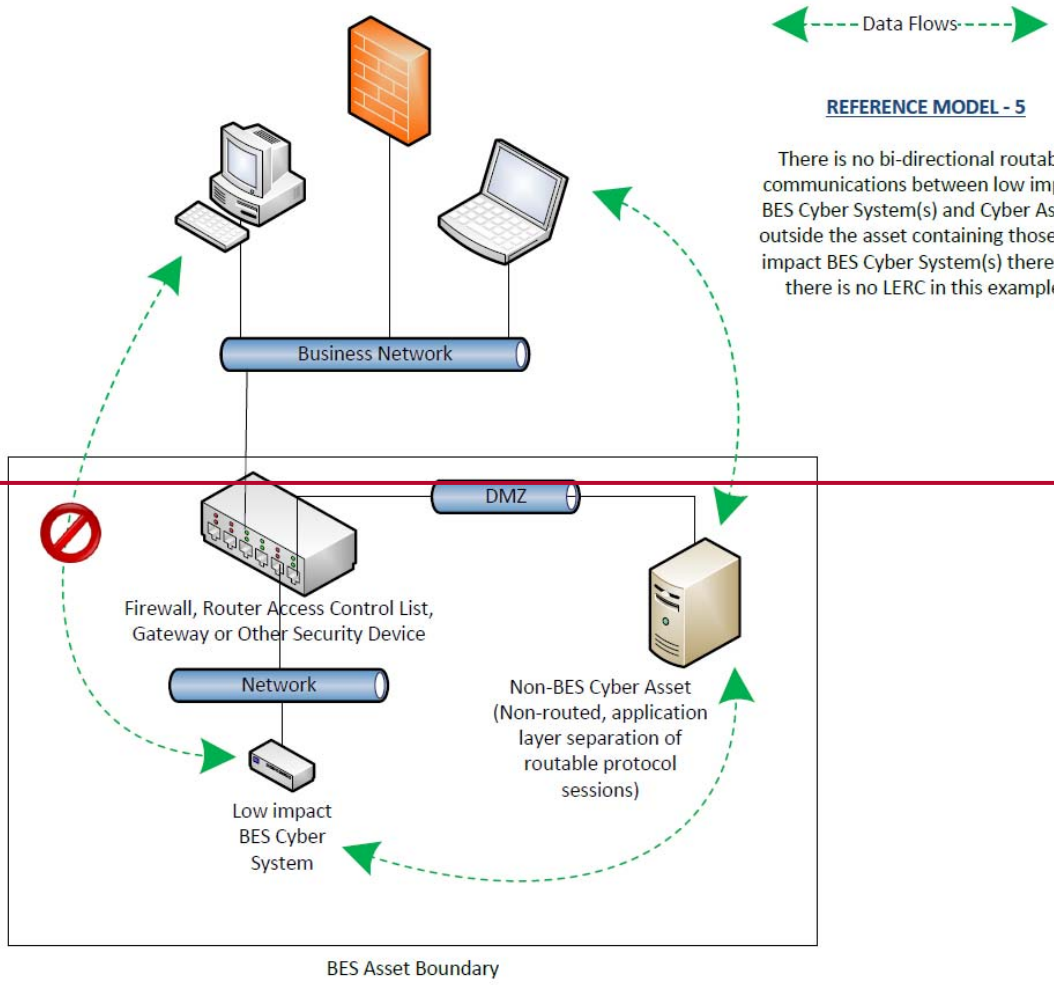

Data Flows
REFERENCE MODEL - 3
The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is place at "Location X" to act as the LEAP(s) and permit only necessary electronic access to the low impact BES Cyber Systems.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Location X
LERC
Network
Non BES Cyber Systsem
Low impact BES Cyber System
BES Asset Boundary
LERC
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

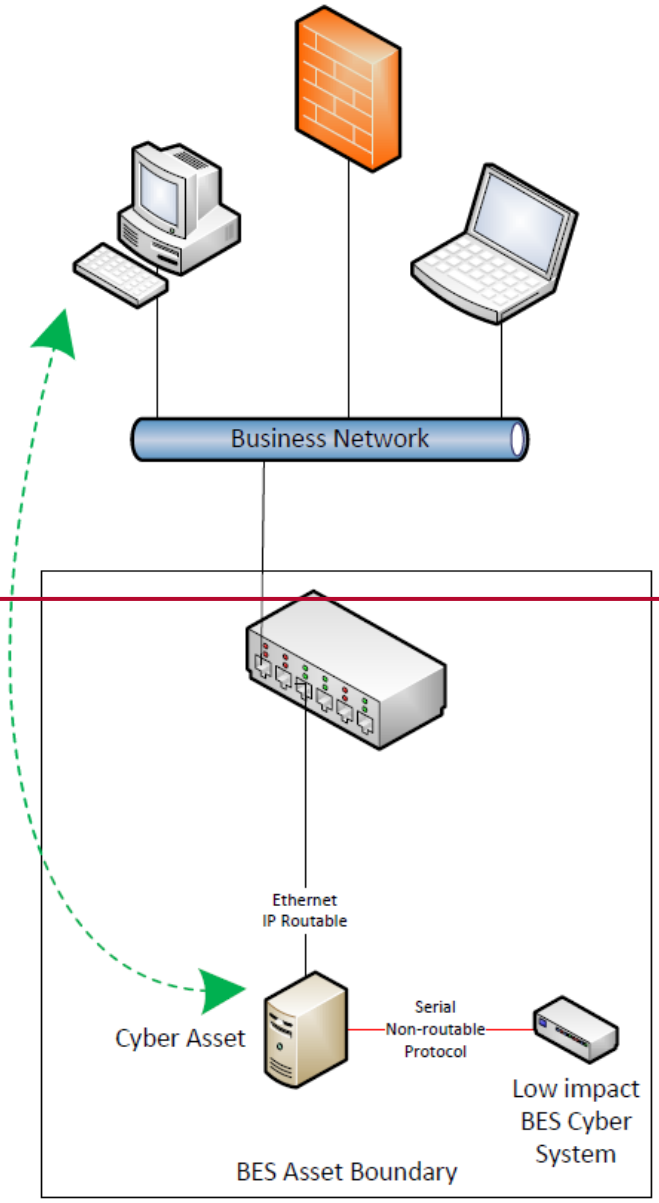


Data Flows

REFERENCE MODEL - 4

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.

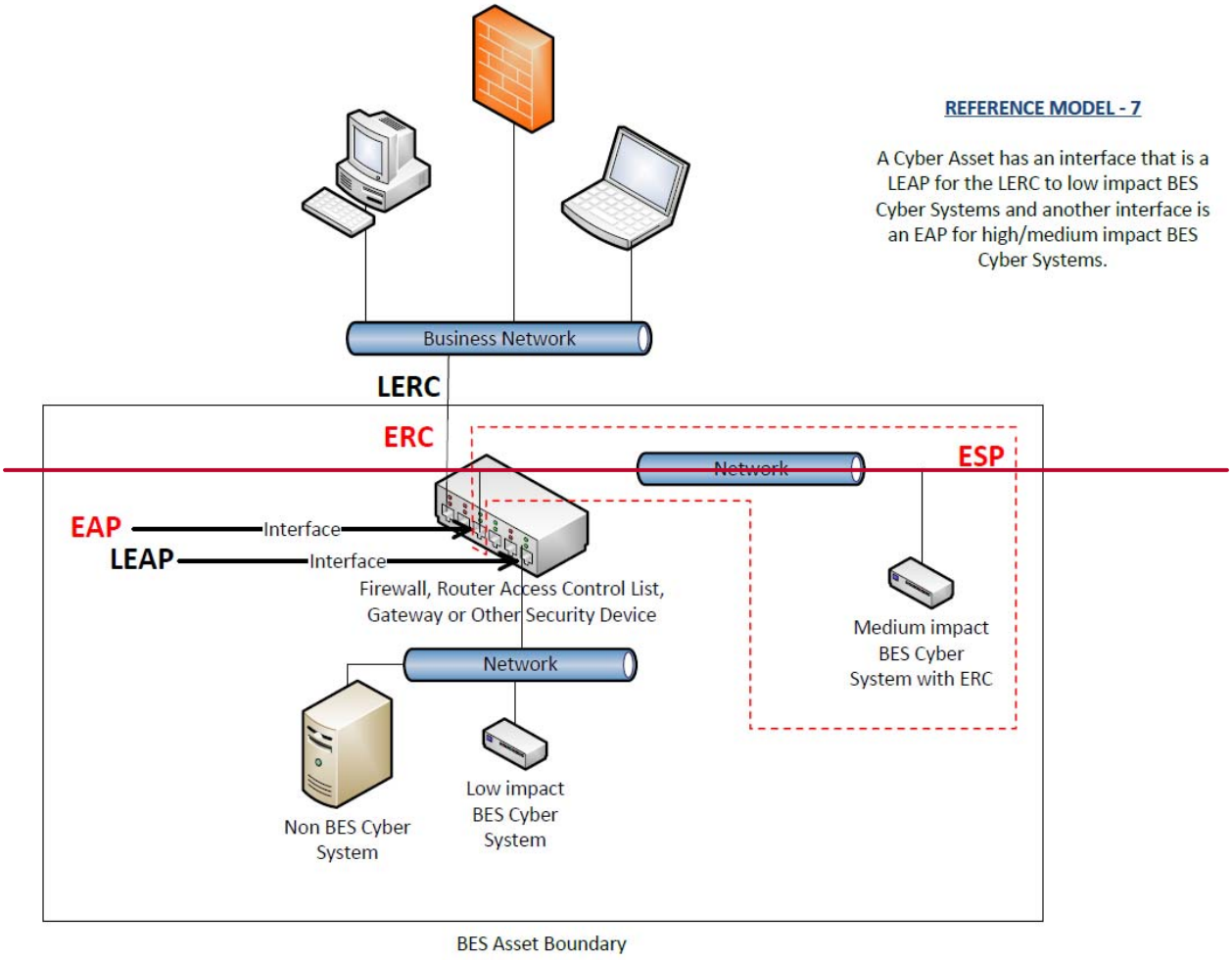

Data Flows
REFERENCE MODEL - 5
There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.
Business Network
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset (Non-routed, application layer separation of routable protocol sessions)
Low impact BES Cyber System
BES Asset Boundary



Data Flows

REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.



Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident

response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-~~6~~7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-~~6~~7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber

Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP

Senior Manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed Revised Term: "Low Impact External Routable Communication" (LERC)

Revised Term: "Low Impact External Routable Communication" (LERC)

Revised Definition:

Routable protocol communication that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), excluding communications between intelligent electronic devices used for time-sensitive protection or control functions between non-Control Center BES assets containing low impact BES Cyber Systems including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols.

Currently Approved Definition of "Low Impact External Routable Connectivity" (LERC):

Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Retire Currently Approved Term "Low Impact BES Cyber System Electronic Access Point" (LEAP):

Given the modified definition of LERC and the proposed modifications in Reliability CIP-003-7, there is no longer a need for the NERC Glossary term *Low Impact BES Cyber System Electronic Access Point* (LEAP):

> A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed Revised Term: "Low Impact External Routable Communication" (LERC)

Revised Term: Low Impact External Routable Communication (LERC)

Revised Definition:

Routable protocol communication that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), excluding communications between intelligent electronic devices used for time-sensitive protection or control functions between non-Control Center BES assets containing low impact BES Cyber Systems including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols.

Redline to Currently Approved Definition: "Low Impact External Routable Connectivity" (LERC)

Routable protocol communication that crosses the boundary of an asset containing one or more~~Direct user-initiated interactive access or a direct device-to-device connection to a~~ low impact BES Cyber System(s), excluding ~~from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point~~ communications between intelligent electronic devices ~~that~~ used ~~routable communication protocols~~ for time-sensitive protection or control functions between non-Control Center BES ~~Transmission station or substation~~ assets containing low impact BES Cyber Systems including,~~are excluded from this definition (examples of this communication include~~ but ~~are~~ not limited to, IEC 61850 GOOSE or vendor proprietary protocols~~)~~.

Currently Approved Definition of "Low Impact External Routable Connectivity" (LERC):

Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Retire Currently Approved Term "Low Impact BES Cyber System Electronic Access Point" (LEAP):

Given the modified definition of LERC and the proposed modifications in Reliability CIP-003-7, there is no longer a need for the NERC Glossary term *Low Impact BES Cyber System Electronic Access Point* (LEAP):

> A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-003-7 Security Management Controls and Low Impact External Routable Communication (LERC)

Requested Approvals

- Reliability Standard CIP-003-7 - Cyber Security – Security Management Controls
- Definition of Low Impact External Routable Communication (LERC)

Requested Retirements

- Reliability Standard CIP-003-6 - Cyber Security – Security Management Controls
- Definition Low Impact BES Cyber System Electronic Access Point (LEAP)
- Definition of Low Impact External Routable Connectivity (LERC)

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards,* approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions. In addition to approving the seven CIP Reliability Standards, the Commission, among other things, directed NERC to modify the definition of LERC. The Commission stated:

> 73. Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity

definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

In addition to modifying the definition consistent with the Commission's directive, the standard drafting team revised the term "LERC" by replacing the word "connectivity" with the word "communication" such that the proposed term for inclusion in the Glossary of Terms used in NERC Reliability Standards (NERC Glossary) is "Low Impact External Routable Communication."

Given the modified definition of LERC and the proposed modifications in Reliability CIP-003-7, there is no longer a need for the NERC Glossary term Low Impact BES Cyber System Electronic Access Point (LEAP). Consequently, NERC is proposing to retire the term LEAP.

General Considerations

This Implementation Plan does not modify the effective date for CIP-003-6 in the Implementation Plan associated with CIP-003-6 nor any of the phased-in compliance dates included therein.

Effective Date

The effective date for the proposed Reliability Standard and NERC Glossary term is provided below:

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7 and the NERC Glossary term *Low Impact External Routable Communication* (LERC) shall become effective on the later of September 1, 2018 or the first day of the first calendar quarter that is nine (9) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-7 and the NERC Glossary term *Low Impact External Routable Communication* (LERC) shall become effective on the first day of the first calendar quarter that is nine (9) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Planned or Unplanned Changes

Planned or Unplanned Changes Resulting in a Higher Categorization – This implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-5 titled Planned or Unplanned Changes Resulting in a Higher Categorization.[1]

Unplanned Changes Resulting in Low Impact Categorization – This implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-6 titled Unplanned Changes Resulting in Low Impact Categorization. That section provides:

[1] Due to the length of that section, it is not reproduced herein.

For unplanned changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

Retirement Date

Reliability Standard CIP-003-6

Reliability Standard CIP-003-6 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-7 in the particular jurisdiction in which the revised standard is becoming effective.

Current NERC Glossary of Terms of LERC and LEAP

The current definition of LERC and the term LEAP shall be retired from the NERC Glossary of Terms immediately prior to the effective date of the revised LERC term in the particular jurisdiction in which the definition is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Modifications to address the FERC directive regarding the Definition of Low Impact External Routable Connectivity

Do not use this form for submitting comments. Use the electronic form to submit comments on the **Modifications to address the Federal Energy Regulatory Commission directive regarding the Definition of Low Impact External Routable Connectivity**. The electronic form must be submitted by **8 p.m. Eastern, Tuesday, September 6, 2016.**

Additional information is available on the project page. If you have questions, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

Background Information

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, Revised Critical Infrastructure Protection Reliability Standards, approving seven CIP Reliability Standards and new or modified definitions. In Order No. 822, the Commission also directed NERC to make certain modifications to those standards and definitions. On March 9, 2016, the NERC Standards Committee authorized the Standards Authorization Request (SAR) to be posted for a 30-day informal comment period from March 23 – April 21, 2016. Based on the comments received, the 2016-02 Modifications to CIP Standards Drafting Team (SDT) made minor revisions to the SAR which was posted for an additional 30-day informal comment period June 1-30, 2016.

In Order 822, the Commission stated:

> "73. Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6."

SDT Approach

The SDT changed the term Low Impact External Routable Connectivity to Low Impact External Routable Communication (LERC) and revised the definition of LERC. The revisions clarify that LERC is an attribute of a BES asset (e.g., a substation or generation facility), not a BES Cyber Asset, and focuses on whether there is routable protocol communications across the asset boundary without regard to 'direct vs. indirect' access that may occur. It removes the dependency between the electronic access controls that may be in

place and having those controls determine whether LERC exists or not. For those BES assets that have LERC, the SDT changed the requirement from requiring a LEAP to requiring electronic access controls to "permit only necessary electronic access to low impact BES Cyber Systems" (revised Attachment 1, Section 3.1) within the BES asset and expanded the Guidelines and Technical Basis with numerous examples of electronic access controls. The proposed definition of LERC is the following:

> **Low Impact External Routable Communication (LERC)** – A routable protocol communication that crosses the boundary of an asset containing one or more low impact BES Cyber Systems, excluding communications between intelligent electronic devices used for time-sensitive protection or control functions between non-Control Center BES assets containing low impact BES Cyber Systems including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols.

With the proposed definition of LERC, the SDT determined that the implemented security controls, which previously created an absence of LERC by making the connection "indirect," would become acceptable methods of electronic access control. As such, the specific implementation of a Low Impact BES Cyber System Electronic Access Point (LEAP) is not required; therefore, the SDT is proposing the retirement of LEAP. This change is reflected in the revised language of CIP-003-7, Attachment 1, Sections 2 and 3.1.

In summary, the SDT made the following changes to address the directive:

1. Revised the definition of LERC
2. Retired Low Impact BES Cyber System Electronic Access Point (LEAP)
3. Revised the requirement language (Requirement R2) of Sections 2 and 3 in Attachment 1 of CIP-003-7
4. Revised the associated High VSL for Requirement R2 of CIP-003-7
5. Revised the evidential language (Measure M2) of Sections 2 and 3 in Attachment 2 of CIP-003-7
6. Non-substantive errata changes within CIP-003-7 such as changing "ES-ISAC" to "E-ISAC".

The SDT requests feedback on the proposed approach to addressing the FERC directive.

Questions

1. Definition: The SDT replaced the term *Low Impact External Routable Connectivity* with *Low Impact External Routable Communication (LERC)* and revised the definition such that it is relevant to the type of communication that occurs crossing the boundary of the BES asset that contains the low impact BES Cyber Systems. This more clearly aligns with the output of CIP-002-5.1 Requirement R1, Part 1.3. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

2. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 2 Physical Security Controls to reflect the retirement of LEAP. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

3. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 3 Electronic Access Controls to require entities to implement electronic access control(s) for LERC, if any, to permit only necessary electronic access to low impact BES Cyber System(s). Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

4. Measure M2: The SDT revised the complementary language of CIP-003-6, Attachment 2, Sections 2 and 3 to make the evidential language of the Measure consistent with the revised requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides **example** diagrams that illustrate various electronic access controls at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

   Yes:

   No:

   Comments:

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) for the revisions made to Sections 2 and 3 of Attachment 2 in CIP-003, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is nine (9) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

7. If you have additional comments on the proposed revisions to address the FERC directive regarding the LERC definition that you have **not** provided in response to the questions above, please provide them here.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 – Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2016-02, Modifications to CIP Standards. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-003-7, Requirement R2	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Lower was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements for low impact BES Cyber Systems. The purpose of plans is for entities to develop an approach involving multiple procedures to address a broad subject matter. Using a plan, Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems.
FERC VRF G1 Discussion Guideline 1 - Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2 - Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement a documented cyber security plan that contains certain sections specified in Attachment 1. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security plan, the VRF is reflective of the plan as a whole. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain low impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3 - Consistency among Reliability Standards	This requirement maps from CIP-003-5, Requirement R1, which has an approved VRF of Medium but applies to Cyber Assets with an inherently lower risk; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Failure to properly implement the cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state

VRF Justifications for CIP-003-7, Requirement R2	
Proposed VRF	**Lower**
Guideline 4 - Consistency with NERC Definitions of VRFs	or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion Guideline 5 - Treatment of Requirements that Co-mingle More than One Obligation	The cyber security plan requirement encompasses a number of subject matter areas for low impact BES Cyber Systems. The VRF is identified at the risk level represented by all of the plan areas in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.

VSLs for CIP-003-7, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems,	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented one or more incident response plans within	The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR	The Responsible Entity failed to document or implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

but failed to document one or more Cyber Security Incident response plans according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2)	its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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. OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to	The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to implement the electronic access controls to low impact BES Cyber Systems according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)	

	Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)		

VSL Justifications for CIP-003-7, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved Requirement R2, CIP-003-6. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-003-7, Requirement R2	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security plan(s) but fails to address one or more of the required sections of Attachment 1. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The action of the requirement is to implement documented cyber security plan(s). Documentation of the plan(s) is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the plan in this case; as such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity implemented all the required elements of the plan. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2016-02 Modifications to CIP Standards

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.	FERC Order 822, Paragraph 73; issued January 21, 2016	The Project 2016-02 Standard Drafting Team (SDT) revised the definition of the term Low Impact External Routable Connectivity to resolve the ambiguity surrounding the term "direct" identified by the Commission. In doing so, the SDT changed the term to Low Impact External Routable *Communication* (LERC) and simplified the definition so that LERC is an attribute of an asset containing low impact BES Cyber Systems. As revised, LERC exists where there is routable protocol communication that crosses the asset boundary without regard to whether 'direct' or 'indirect' access may occur. The revised LERC definition removes the dependency between the electronic access controls that may be in place and having those controls determine whether LERC exists or not. The SDT determined that indirect access, regardless of what kind of 'security break' is in place causing it to be indirect, is another form of electronic access control that is intended to meet the same security objective. The SDT determined that the requirements should address the electronic access controls rather than having some controls implied through the definition. Therefore, for those assets containing low impact BES Cyber Systems that have

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		LERC, the SDT changed the language in Attachment 1, Section 3.1 from requiring a Low Impact Electronic Access Point (LEAP) to requiring that electronic access controls be implemented to meet the security objective of permitting "only necessary electronic access to low impact BES Cyber Systems." Additionally, the SDT expanded the Guidelines and Technical Basis with numerous examples of electronic access control concepts that accomplish this objective. Given the modified definition of LERC and the proposed modifications in Reliability CIP-003-7, there is no longer a need for the NERC Glossary term Low Impact BES Cyber System Electronic Access Point (LEAP). Consequently, the SDT proposed the term's retirement.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Reminder

Project 2016-02 Modifications to CIP Standards

Initial Ballots and Non-binding Poll Open through September 6, 2016

Now Available

The following ballots are open through **8 p.m. Eastern, Tuesday, September 6, 2016**:

1. **Initial ballot for CIP-003-7 - Cyber Security – Security Management Controls**
2. **Initial ballot for CIP-003-7 Implementation Plan**
3. **Initial ballot for the new term - Low Impact External Routable Communication (LERC) and its definition**
4. **Non-binding poll of the associated Violation Risk Factors and Violation Severity Levels**

Balloting

Members of the ballot pools associated with this project may log in and submit their vote for the standard and its implementation plan, the new term LERC and its definition, and the non-binding poll by clicking here. If you experience any difficulties in using the electronic form, contact Wendy Muller.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Al McMeekin at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Period Open through September 6, 2016
Ballot Pools Forming through August 19, 2016

Now Available

A 45-day formal comment period is open through **8 p.m. Eastern, Monday, September 6, 2016** for:

1. **CIP-003-7 - Cyber Security – Security Management Controls**
2. **CIP-003-7 implementation plan**
3. **The new term - Low Impact External Routable Communication (LERC) and its definition**

Commenting

Use the electronic form to submit comments. If you experience any difficulties using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

Join the Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Friday, August 19, 2016.** Registered Ballot Body members may join the ballot pools here.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 8 p.m. Eastern).

Next Steps

Initial ballots for the standard, implementation plan, and the new term for and definition of LERC, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **August 26 – September 6, 2016**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/61)
Ballot Name: 2016-02 Modifications to CIP Standards CIP-003-7 IN 1 ST
Voting Start Date: 8/26/2016 12:01:00 AM
Voting End Date: 9/6/2016 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 289
Total Ballot Pool: 340
Quorum: 85
Weighted Segment Value: 41.54

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	25	0.362	44	0.638	0	5	12
Segment: 2	8	0.3	2	0.2	1	0.1	0	3	2
Segment: 3	75	1	23	0.365	40	0.635	0	1	11
Segment: 4	26	1	7	0.318	15	0.682	0	0	4
Segment: 5	80	1	21	0.323	44	0.677	0	0	15
Segment: 6	48	1	9	0.214	33	0.786	1	1	4
Segment: 7	3	0.1	0	0	1	0.1	0	0	2
Segment: 8	3	0.2	2	0.2	0	0	0	0	1
Segment: 9	2	0.2	1	0.1	1	0.1	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.9	7	0.7	2	0.2	0	0	0
Totals:	340	6.7	97	2.783	181	3.917	1	10	51

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Negative	Comments Submitted
1	Ameren - Ameren Services	Eric Scott		Negative	Third-Party Comments
1	American Transmission Company, LLC	Andrew Pusztai		Abstain	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Third-Party Comments
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	Negative	Third-Party Comments
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Wes Wingen		Negative	Third-Party Comments
1	Bonneville Power Administration	Donald Watkins		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Third-Party Comments
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	Third-Party Comments
1	CMS Energy - Consumers Energy Company	Bruce Bugbee		Affirmative	N/A
1	Colorado Springs Utilities	Devin Elverdi		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		None	N/A
1	Duke Energy	Doug Hils		Negative	Third-Party Comments
1	Edison International - Southern California Edison Company	Steven Mavis		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Empire District Electric Co.	Ralph Meyer		None	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass	Matt Stryker	Negative	Comments Submitted
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Negative	Comments Submitted
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Johnny Anderson		Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Abstain	N/A
1	JEA	Ted Hobson	Joe McClung	Negative	Third-Party Comments
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		Negative	Third-Party Comments
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Teresa Cantwell		Abstain	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Negative	Third-Party Comments
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A
1	Platte River Power Authority	Matt Thompson		Negative	Comments Submitted
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Negative	Third-Party Comments
1	Portland General Electric Co.	Scott Smith		Negative	Third-Party Comments
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Negative	Third-Party Comments
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Third-Party Comments
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Negative	Comments Submitted
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Third-Party Comments
1	Salt River Project	Steven Cobb		Negative	Comments Submitted
1	Santee Cooper	Shawn Abrams		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	Negative	Third-Party Comments
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Martine Blair		None	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A
1	Tennessee Valley Authority	Howell Scott		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Negative	Third-Party Comments
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	BC Hydro and Power Authority	Venkataramakrishnan Vinnakota		Abstain	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Third-Party Comments
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Negative	Third-Party Comments
3	Anaheim Public Utilities Dept.	Dennis Schmidt		None	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Negative	Comments Submitted
3	Arkansas Electric Cooperative Corporation	Philip Huff		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Julie Ross		Negative	Comments Submitted
3	Avista - Avista Corporation	Scott Kinney		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Third-Party Comments
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		Negative	Comments Submitted
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Negative	Third-Party Comments
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Third-Party Comments
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Empire District Electric Co.	Kalem Long		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	Comments Submitted
3	Gainesville Regional Utilities	Ken Simmons		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Negative	Comments Submitted
3	Great River Energy	Brian Glover		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Oshani Pathirane	Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Third-Party Comments
3	Los Angeles Department of Water and Power	Mike Anctil		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Negative	Third-Party Comments
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		None	N/A
3	Platte River Power Authority	Jeff Landis		Negative	Comments Submitted
3	PNM Resources	Michael Mertz		Negative	Third-Party Comments
3	Portland General Electric Co.	Angela Gaines		Negative	Third-Party Comments
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Negative	Comments Submitted
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Andrea Basinski		Negative	Third-Party Comments
3	Salt River Project	Rudy Navarro		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Negative	Third-Party Comments
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	None	N/A
3	Snohomish County PUD No. 1	Mark Oens		Negative	Third-Party Comments
3	Southern Company - Alabama Power Company	R. Scott Moore		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		None	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	Third-Party Comments
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Bo Jones		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Michael Ibold		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		None	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		None	N/A
4	Austin Energy	Tina Garvey		Negative	Comments Submitted
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		Affirmative	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	Comments Submitted
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Negative	Comments Submitted
4	Georgia System Operations Corporation	Guy Andrews		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Illinois Municipal Electric Agency	Bob Thomas		Negative	Third-Party Comments
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	Negative	Third-Party Comments
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Negative	Comments Submitted
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Negative	Third-Party Comments
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Third-Party Comments
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Negative	Third-Party Comments
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	Comments Submitted
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Third-Party Comments
5	APS - Arizona Public Service Co.	Stephanie Little		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Matthew Finn		Affirmative	N/A
5	Austin Energy	Jeanie Doty		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Negative	Third-Party Comments
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Negative	Comments Submitted
5	Black Hills Corporation	George Tatar		Negative	Third-Party Comments
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Third-Party Comments
5	Bonneville Power Administration	Francis Halpin		Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Third-Party Comments
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Third-Party Comments
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Third-Party Comments
5	EDP Renewables North America LLC	Heather Morgan		Affirmative	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Negative	Comments Submitted
5	Great River Energy	Preston Walsh		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Negative	Third-Party Comments
5	Hydro-Qu?bec Production	Roger Dufresne		Negative	Comments Submitted
5	JEA	John Babik		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Kissimmee Utility Authority	Mike Blough		Negative	Third-Party Comments
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Third-Party Comments
5	Los Angeles Department of Water and Power	Kenneth Silver		Affirmative	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Rick Terrill		Negative	Third-Party Comments
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Negative	Comments Submitted
5	MEAG Power	Steven Grego	Scott Miller	Negative	Third-Party Comments
5	Muscatine Power and Water	Mike Avesing		None	N/A
5	Nebraska Public Power District	Don Schmit		Negative	Third-Party Comments
5	New York Power Authority	Wayne Sipperly		Affirmative	N/A
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	Leo Staples		Negative	Third-Party Comments
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		None	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Negative	Third-Party Comments
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Negative	Comments Submitted
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Third-Party Comments
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Lynda Kupfer		Negative	Third-Party Comments
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seattle City Light	Mike Haynes		Negative	Third-Party Comments
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Negative	Comments Submitted
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Negative	Third-Party Comments
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	Tri-State G and T Association, Inc.	Mark Stein		None	N/A
5	U.S. Bureau of Reclamation	Erika Doot		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Negative	Comments Submitted
5	Westar Energy	stephanie johnson		Negative	Third-Party Comments
5	Xcel Energy, Inc.	David Lemmons		Negative	Third-Party Comments
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	APS - Arizona Public Service Co.	Bobbi Welch		Negative	Comments Submitted
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		None	N/A
6	Austin Energy	Andrew Gallo		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Bonneville Power Administration	Alex Spain		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Third-Party Comments
6	Colorado Springs Utilities	Shannon Fair		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston	Dermot Smyth	Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Third-Party Comments
6	Entergy	Julie Hall		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	Comments Submitted
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Negative	Comments Submitted
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Third-Party Comments
6	Lincoln Electric System	Eric Ruskamp		Negative	Third-Party Comments
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Lower Colorado River Authority	Michael Shaw		Abstain	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Negative	Third-Party Comments
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Negative	Third-Party Comments
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		None	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Portland General Electric Co.	Adam Menendez		Negative	Third-Party Comments
6	Powerex Corporation	Gordon Dobson-Mack		Negative	No Comment Submitted
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Comments Submitted
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Negative	Comments Submitted
6	Salt River Project	William Abraham		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
6	Seattle City Light	Charles Freeman		Negative	Third-Party Comments
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Negative	Third-Party Comments
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Elizabeth Davis		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	Third-Party Comments
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	Westar Energy	Megan Wagner		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Exxon Mobil	Jay Barnett		Negative	Comments Submitted
7	Luminant Mining Company LLC	Stewart Rake		None	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		None	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	Comments Submitted
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		Negative	Comments Submitted
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 340 of 340 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/61)
Ballot Name: 2016-02 Modifications to CIP Standards CIP-003-7 Implementation Plan IN 1 OT
Voting Start Date: 8/26/2016 12:01:00 AM
Voting End Date: 9/6/2016 8:00:00 PM
Ballot Type: OT
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 286
Total Ballot Pool: 339
Quorum: 84.37
Weighted Segment Value: 41.77

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	30	0.435	39	0.565	0	4	12
Segment: 2	8	0.2	2	0.2	0	0	0	4	2
Segment: 3	75	1	25	0.397	38	0.603	0	1	11
Segment: 4	26	1	8	0.381	13	0.619	0	0	5
Segment: 5	80	1	24	0.375	40	0.625	0	0	16
Segment: 6	48	1	12	0.286	30	0.714	1	1	4
Segment: 7	3	0	0	0	0	0	0	1	2
Segment: 8	3	0.2	2	0.2	0	0	0	0	1
Segment: 9	2	0.2	0	0	2	0.2	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.8	4	0.4	4	0.4	0	1	0
Totals:	339	6.4	107	2.673	166	3.727	1	12	53

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Negative	Third-Party Comments
1	American Transmission Company, LLC	Andrew Pusztai		Abstain	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Third-Party Comments
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	Negative	Third-Party Comments
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Bonneville Power Administration	Donald Watkins		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Third-Party Comments
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	Third-Party Comments
1	CMS Energy - Consumers Energy Company	Bruce Bugbee		Affirmative	N/A
1	Colorado Springs Utilities	Devin Elverdi		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		None	N/A
1	Duke Energy	Doug Hils		Negative	Third-Party Comments
1	Edison International - Southern California Edison Company	Steven Mavis		None	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass	Matt Stryker	Negative	Comments Submitted
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Negative	Comments Submitted
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Johnny Anderson		Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Negative	Third-Party Comments
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Teresa Cantwell		Abstain	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Negative	Third-Party Comments
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Negative	Third-Party Comments
1	Portland General Electric Co.	Scott Smith		Negative	Third-Party Comments
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Negative	Third-Party Comments
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Third-Party Comments
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Third-Party Comments
1	Salt River Project	Steven Cobb		Negative	Comments Submitted
1	Santee Cooper	Shawn Abrams		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	Negative	Third-Party Comments
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Martine Blair		None	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A
1	Tennessee Valley Authority	Howell Scott		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Tracy Sliman		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Negative	Third-Party Comments
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	BC Hydro and Power Authority	Venkataramakrishnan Vinnakota		Abstain	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Negative	Third-Party Comments
3	Anaheim Public Utilities Dept.	Dennis Schmidt		None	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Negative	Comments Submitted
3	Arkansas Electric Cooperative Corporation	Philip Huff		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Julie Ross		Negative	Comments Submitted
3	Avista - Avista Corporation	Scott Kinney		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Third-Party Comments
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		Negative	Comments Submitted
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Third-Party Comments
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Exelon	John Bee		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	Comments Submitted
3	Gainesville Regional Utilities	Ken Simmons		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Negative	Comments Submitted
3	Great River Energy	Brian Glover		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Oshani Pathirane	Negative	Comments Submitted
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Negative	Third-Party Comments
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		None	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Negative	Third-Party Comments
3	Portland General Electric Co.	Angela Gaines		Negative	Third-Party Comments
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Negative	Comments Submitted
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Andrea Basinski		Negative	Third-Party Comments
3	Salt River Project	Rudy Navarro		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Negative	Third-Party Comments
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	None	N/A
3	Snohomish County PUD No. 1	Mark Oens		Negative	Third-Party Comments
3	Southern Company - Alabama Power Company	R. Scott Moore		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		None	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	Third-Party Comments
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Bo Jones		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Michael Ibold		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		None	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		None	N/A
4	Austin Energy	Tina Garvey		Negative	Comments Submitted
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		Affirmative	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	Comments Submitted
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Negative	Comments Submitted
4	Georgia System Operations Corporation	Guy Andrews		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	Negative	Third-Party Comments
4	LaGen	Richard Comeaux		Negative	Comments Submitted
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Negative	Comments Submitted
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Third-Party Comments
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Third-Party Comments
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	Comments Submitted
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Third-Party Comments
5	APS - Arizona Public Service Co.	Stephanie Little		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Matthew Finn		Affirmative	N/A
5	Austin Energy	Jeanie Doty		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Negative	Third-Party Comments
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Negative	Comments Submitted
5	Black Hills Corporation	George Tatar		Negative	Third-Party Comments
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Third-Party Comments
5	Bonneville Power Administration	Francis Halpin		Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Third-Party Comments
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Third-Party Comments
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Third-Party Comments
5	EDP Renewables North America LLC	Heather Morgan		Affirmative	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Negative	Comments Submitted
5	Great River Energy	Preston Walsh		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Negative	Third-Party Comments
5	Hydro-Qu?bec Production	Roger Dufresne		Negative	Comments Submitted
5	JEA	John Babik		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Kissimmee Utility Authority	Mike Blough		Negative	Third-Party Comments
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Affirmative	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Rick Terrill		Negative	Third-Party Comments
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Negative	Third-Party Comments
5	Muscatine Power and Water	Mike Avesing		None	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Erick Barrios		None	N/A
5	NextEra Energy	Allen Schriver		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Leo Staples		Negative	Third-Party Comments
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		None	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Negative	Comments Submitted
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Third-Party Comments
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer		Negative	Third-Party Comments
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	Seattle City Light	Mike Haynes		Negative	Third-Party Comments
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Negative	Comments Submitted
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Negative	Comments Submitted
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Negative	Third-Party Comments
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	Tri-State G and T Association, Inc.	Mark Stein		None	N/A
5	U.S. Bureau of Reclamation	Erika Doot		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Negative	Comments Submitted
5	Westar Energy	stephanie johnson		Negative	Third-Party Comments
5	Xcel Energy, Inc.	David Lemmons		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Third-Party Comments
6	APS - Arizona Public Service Co.	Bobbi Welch		Negative	Comments Submitted
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		None	N/A
6	Austin Energy	Andrew Gallo		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Bonneville Power Administration	Alex Spain		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Third-Party Comments
6	Colorado Springs Utilities	Shannon Fair		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston	Dermot Smyth	Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	Third-Party Comments
6	Entergy	Julie Hall		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Negative	Comments Submitted
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Third-Party Comments
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Lower Colorado River Authority	Michael Shaw		Abstain	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Negative	Third-Party Comments
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Negative	Third-Party Comments
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		None	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Adam Menendez		Negative	Third-Party Comments
6	Powerex Corporation	Gordon Dobson-Mack		Negative	No Comment Submitted
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Comments Submitted
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Negative	Comments Submitted
6	Salt River Project	William Abraham		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
6	Seattle City Light	Charles Freeman		Negative	Third-Party Comments
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Negative	Third-Party Comments
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Elizabeth Davis		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	Third-Party Comments
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Westar Energy	Megan Wagner		Negative	Third-Party Comments
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Exxon Mobil	Jay Barnett		Abstain	N/A
7	Luminant Mining Company LLC	Stewart Rake		None	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		None	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	Comments Submitted
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Negative	Third-Party Comments
10	Florida Reliability Coordinating Council	Peter Heidrich		Abstain	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		Negative	Comments Submitted
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 339 of 339 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/61)
Ballot Name: 2016-02 Modifications to CIP Standards Low Impact External Routable Communication | New Term/Definition IN 1 DEF
Voting Start Date: 8/26/2016 12:01:00 AM
Voting End Date: 9/6/2016 8:00:00 PM
Ballot Type: DEF
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 286
Total Ballot Pool: 338
Quorum: 84.62
Weighted Segment Value: 30.63

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	84	1	21	0.309	47	0.691	0	4	12
Segment: 2	8	0.2	2	0.2	0	0	0	4	2
Segment: 3	74	1	21	0.333	42	0.667	0	1	10
Segment: 4	26	1	5	0.227	17	0.773	0	0	4
Segment: 5	81	1	18	0.277	47	0.723	0	0	16
Segment: 6	48	1	9	0.214	33	0.786	1	1	4
Segment: 7	3	0.1	0	0	1	0.1	0	0	2
Segment: 8	3	0.2	0	0	2	0.2	0	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	2	0.2	0	0	2	0.2	0	0	0
Segment: 10	9	0.7	4	0.4	3	0.3	0	1	1
Totals:	338	6.4	80	1.961	194	4.439	1	11	52

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Negative	Comments Submitted
1	Ameren - Ameren Services	Eric Scott		Negative	Third-Party Comments
1	American Transmission Company, LLC	Andrew Pusztai		Abstain	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Third-Party Comments
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Bonneville Power Administration	Donald Watkins		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Third-Party Comments
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	Third-Party Comments
1	CMS Energy - Consumers Energy Company	Bruce Bugbee		Affirmative	N/A
1	Colorado Springs Utilities	Devin Elverdi		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Negative	Comments Submitted
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		None	N/A
1	Duke Energy	Doug Hils		Negative	Third-Party Comments
1	Edison International - Southern California Edison Company	Steven Mavis		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Empire District Electric Co.	Ralph Meyer		None	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass	Matt Stryker	Negative	Comments Submitted
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Negative	Comments Submitted
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Johnny Anderson		Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Negative	Third-Party Comments
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		Negative	Third-Party Comments
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Lower Colorado River Authority	Teresa Cantwell		Abstain	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Negative	Third-Party Comments
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		None	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A
1	Platte River Power Authority	Matt Thompson		Negative	Comments Submitted
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Negative	Third-Party Comments
1	Portland General Electric Co.	Scott Smith		Negative	Third-Party Comments
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Negative	Third-Party Comments
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Third-Party Comments
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Negative	Comments Submitted
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Third-Party Comments
1	Salt River Project	Steven Cobb		Negative	Comments Submitted
1	Santee Cooper	Shawn Abrams		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	Negative	Third-Party Comments
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Martine Blair		None	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A
1	Tennessee Valley Authority	Howell Scott		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Negative	Third-Party Comments
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	BC Hydro and Power Authority	Venkataramakrishnan Vinnakota		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Negative	Third-Party Comments
3	APS - Arizona Public Service Co.	Jeri Freimuth		Negative	Comments Submitted
3	Arkansas Electric Cooperative Corporation	Philip Huff		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Julie Ross		Negative	Comments Submitted
3	Avista - Avista Corporation	Scott Kinney		Negative	Third-Party Comments
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Third-Party Comments
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		Negative	Comments Submitted
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Third-Party Comments
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Cowlitz County PUD	Russell Noble		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	Comments Submitted
3	Gainesville Regional Utilities	Ken Simmons		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Negative	Comments Submitted
3	Great River Energy	Brian Glover		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Oshani Pathirane	Negative	Comments Submitted
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Third-Party Comments
3	Los Angeles Department of Water and Power	Mike Anctil		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Negative	Third-Party Comments
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		None	N/A
3	Platte River Power Authority	Jeff Landis		Negative	Comments Submitted
3	PNM Resources	Michael Mertz		Negative	Third-Party Comments
3	Portland General Electric Co.	Angela Gaines		Negative	Third-Party Comments
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Negative	Comments Submitted
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Andrea Basinski		Negative	Third-Party Comments
3	Salt River Project	Rudy Navarro		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Negative	Third-Party Comments
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	None	N/A
3	Snohomish County PUD No. 1	Mark Oens		Negative	Third-Party Comments
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		None	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	Third-Party Comments
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Bo Jones		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Michael Ibold		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		None	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		None	N/A
4	Austin Energy	Tina Garvey		Negative	Comments Submitted
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		Affirmative	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	Comments Submitted
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Negative	Comments Submitted
4	Georgia System Operations Corporation	Guy Andrews		Negative	Comments Submitted
4	Illinois Municipal Electric Agency	Bob Thomas		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	Negative	Third-Party Comments
4	LaGen	Richard Comeaux		Negative	Comments Submitted
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Negative	Comments Submitted
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Negative	Third-Party Comments
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Third-Party Comments
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Negative	Third-Party Comments
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	Comments Submitted
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Comments Submitted
5	AEP	Thomas Foltz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Third-Party Comments
5	APS - Arizona Public Service Co.	Stephanie Little		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Matthew Finn		Affirmative	N/A
5	Austin Energy	Jeanie Doty		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Negative	Third-Party Comments
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Negative	Comments Submitted
5	Black Hills Corporation	George Tatar		Negative	Third-Party Comments
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Third-Party Comments
5	Bonneville Power Administration	Francis Halpin		Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Third-Party Comments
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Third-Party Comments
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Mike Hirst		None	N/A
5	Colorado Springs Utilities	Jeff Icke		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Third-Party Comments
5	EDP Renewables North America LLC	Heather Morgan		Affirmative	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Negative	Comments Submitted
5	Great River Energy	Preston Walsh		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Negative	Third-Party Comments
5	Hydro-Qu?bec Production	Roger Dufresne		Negative	Comments Submitted
5	JEA	John Babik		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Kissimmee Utility Authority	Mike Blough		Negative	Third-Party Comments
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Third-Party Comments
5	Los Angeles Department of Water and Power	Kenneth Silver		Affirmative	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Rick Terrill		Negative	Third-Party Comments
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Negative	Comments Submitted
5	MEAG Power	Steven Grego	Scott Miller	Negative	Third-Party Comments
5	Muscatine Power and Water	Mike Avesing		None	N/A
5	Nebraska Public Power District	Don Schmit		Negative	Third-Party Comments
5	New York Power Authority	Wayne Sipperly		Negative	Third-Party Comments
5	NextEra Energy	Allen Schriver		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Leo Staples		Negative	Third-Party Comments
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		None	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Negative	Third-Party Comments
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Negative	Comments Submitted
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Third-Party Comments
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Lynda Kupfer		Negative	Third-Party Comments
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	Seattle City Light	Mike Haynes		Negative	Third-Party Comments
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Negative	Comments Submitted
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Negative	Third-Party Comments
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	Tri-State G and T Association, Inc.	Mark Stein		None	N/A
5	U.S. Bureau of Reclamation	Erika Doot		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Negative	Comments Submitted
5	Westar Energy	stephanie johnson		Negative	Third-Party Comments
5	Xcel Energy, Inc.	David Lemmons		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Third-Party Comments
6	APS - Arizona Public Service Co.	Bobbi Welch		Negative	Comments Submitted
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		None	N/A
6	Austin Energy	Andrew Gallo		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Bonneville Power Administration	Alex Spain		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Third-Party Comments
6	Colorado Springs Utilities	Shannon Fair		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston	Dermot Smyth	Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	Third-Party Comments
6	Entergy	Julie Hall		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Negative	Comments Submitted
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Third-Party Comments
6	Lincoln Electric System	Eric Ruskamp		Negative	Third-Party Comments
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Lower Colorado River Authority	Michael Shaw		Abstain	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Negative	Third-Party Comments
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Negative	Third-Party Comments
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		None	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Negative	Comments Submitted
6	Portland General Electric Co.	Adam Menendez		Negative	Third-Party Comments
6	Powerex Corporation	Gordon Dobson-Mack		Negative	No Comment Submitted
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Comments Submitted
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Negative	Comments Submitted
6	Salt River Project	William Abraham		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
6	Seattle City Light	Charles Freeman		Negative	Third-Party Comments
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Negative	Third-Party Comments
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Elizabeth Davis		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	Third-Party Comments
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Westar Energy	Megan Wagner		Negative	Third-Party Comments
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Exxon Mobil	Jay Barnett		Negative	Comments Submitted
7	Luminant Mining Company LLC	Stewart Rake		None	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments
8	Massachusetts Attorney General	Frederick Plett		Negative	Third-Party Comments
8	Roger Zaklukiewicz	Roger Zaklukiewicz		None	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	Comments Submitted
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Negative	Third-Party Comments
10	Florida Reliability Coordinating Council	Peter Heidrich		Abstain	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 338 of 338 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/61)
Ballot Name: 2016-02 Modifications to CIP Standards CIP-003-7 Non-binding Poll IN 1 NB
Voting Start Date: 8/26/2016 12:01:00 AM
Voting End Date: 9/6/2016 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 267
Total Ballot Pool: 321
Quorum: 83.18
Weighted Segment Value: 37.73

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	21	0.375	35	0.625	13	11
Segment: 2	8	0.2	2	0.2	0	0	4	2
Segment: 3	75	1	22	0.423	30	0.577	10	13
Segment: 4	23	1	5	0.313	11	0.688	3	4
Segment: 5	73	1	16	0.333	32	0.667	10	15
Segment: 6	45	1	7	0.212	26	0.788	7	5
Segment: 7	3	0.1	0	0	1	0.1	0	2
Segment: 8	3	0.2	2	0.2	0	0	0	1
Segment: 9	2	0.2	1	0.1	1	0.1	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	9	0.8	7	0.7	1	0.1	0	1
Totals:	321	6.5	83	2.856	137	3.644	47	54

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Negative	Comments Submitted
1	Ameren - Ameren Services	Eric Scott		Negative	Comments Submitted
1	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Bonneville Power Administration	Donald Watkins		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Abstain	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	Comments Submitted
1	CMS Energy - Consumers Energy Company	Bruce Bugbee		Affirmative	N/A
1	Colorado Springs Utilities	Devin Elverdi		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		None	N/A
1	Duke Energy	Doug Hils		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		None	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass	Matt Stryker	Negative	Comments Submitted
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Negative	Comments Submitted
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Johnny Anderson		Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Danny Pudenz		Abstain	N/A
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Teresa Cantwell		Abstain	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	Scott Miller	Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat		Abstain	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		None	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Abstain	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Negative	Comments Submitted
1	Portland General Electric Co.	Scott Smith		Negative	Comments Submitted
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Abstain	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Negative	Comments Submitted
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Comments Submitted
1	Salt River Project	Steven Cobb		Negative	Comments Submitted
1	Santee Cooper	Shawn Abrams		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	Negative	Third-Party Comments
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Martine Blair		None	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A
1	Tennessee Valley Authority	Howell Scott		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Negative	Comments Submitted
1	Western Area Power Administration	sean erickson		Abstain	N/A
2	BC Hydro and Power Authority	Venkataramakrishnan Vinnakota		Abstain	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	Midcontinent ISO, Inc.	Terry Bllke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		None	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Negative	Comments Submitted
3	Arkansas Electric Cooperative Corporation	Philip Huff		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Julie Ross		Negative	Comments Submitted
3	Avista - Avista Corporation	Scott Kinney		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		Negative	Comments Submitted
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Abstain	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Abstain	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	Comments Submitted
3	Gainesville Regional Utilities	Ken Simmons		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great River Energy	Brian Glover		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Oshani Pathirane	Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		None	N/A
3	Platte River Power Authority	Jeff Landis		Negative	Comments Submitted
3	PNM Resources	Michael Mertz		Negative	Comments Submitted
3	Portland General Electric Co.	Angela Gaines		Negative	Comments Submitted
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Abstain	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Andrea Basinski		Negative	Comments Submitted
3	Salt River Project	Rudy Navarro		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	None	N/A
3	Snohomish County PUD No. 1	Mark Oens		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	R. Scott Moore		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Abstain	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		None	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Bo Jones		Negative	Comments Submitted
3	Xcel Energy, Inc.	Michael Ibold		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		None	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		None	N/A
4	Austin Energy	Tina Garvey		Negative	Comments Submitted
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		Affirmative	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	Comments Submitted
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Negative	Comments Submitted
4	Georgia System Operations Corporation	Guy Andrews		Negative	Comments Submitted
4	Illinois Municipal Electric Agency	Bob Thomas		Abstain	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	Negative	Comments Submitted
4	LaGen	Richard Comeaux		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Negative	Third-Party Comments
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Abstain	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Comments Submitted
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Matthew Finn		Affirmative	N/A
5	Austin Energy	Jeanie Doty		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Abstain	N/A
5	Black Hills Corporation	George Tatar		Negative	Third-Party Comments
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Comments Submitted
5	Bonneville Power Administration	Francis Halpin		Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Comments Submitted
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Abstain	N/A
5	Colorado Springs Utilities	Jeff Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		Affirmative	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Negative	Comments Submitted
5	Great River Energy	Preston Walsh		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Herb Schrayshuen	Herb Schrayshuen		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Roger Dufresne		None	N/A
5	JEA	John Babik		Negative	Comments Submitted
5	Kissimmee Utility Authority	Mike Blough		Negative	Comments Submitted
5	Lakeland Electric	Jim Howard		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Abstain	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Rick Terrill		Negative	Comments Submitted
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Abstain	N/A
5	MEAG Power	Steven Grego	Scott Miller	Negative	Comments Submitted
5	Muscatine Power and Water	Mike Avesing		None	N/A
5	Nebraska Public Power District	Don Schmit		Abstain	N/A
5	New York Power Authority	Wayne Sipperly		Affirmative	N/A
5	NextEra Energy	Allen Schriver		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Leo Staples		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Lynda Kupfer		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	Seattle City Light	Mike Haynes		Negative	Third-Party Comments
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Negative	Comments Submitted
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Abstain	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Abstain	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		None	N/A
5	U.S. Bureau of Reclamation	Erika Doot		Negative	Comments Submitted
5	Westar Energy	stephanie johnson		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Negative	Comments Submitted
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Associated Electric Cooperative, Inc.	Brian Ackermann		None	N/A
6	Austin Energy	Andrew Gallo		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Bonneville Power Administration	Alex Spain		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Comments Submitted
6	Colorado Springs Utilities	Shannon Fair		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston	Dermot Smyth	Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Entergy	Julie Hall		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	Comments Submitted
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Negative	Comments Submitted
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Lower Colorado River Authority	Michael Shaw		Abstain	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Negative	Comments Submitted
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		None	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Comments Submitted
6	Portland General Electric Co.	Adam Menendez		Negative	Comments Submitted
6	Powerex Corporation	Gordon Dobson-Mack		Negative	Comments Submitted
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Salt River Project	William Abraham		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
6	Seattle City Light	Charles Freeman		Negative	Third-Party Comments
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Negative	Comments Submitted
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Abstain	N/A
6	Talen Energy Marketing, LLC	Elizabeth Davis		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	Westar Energy	Megan Wagner		Negative	Comments Submitted
7	Exxon Mobil	Jay Barnett		Negative	Comments Submitted
7	Luminant Mining Company LLC	Stewart Rake		None	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	Comments Submitted
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 321 of 321 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Period Open through September 6, 2016
Ballot Pools Forming through August 19, 2016

Now Available

A 45-day formal comment period is open through **8 p.m. Eastern, Monday, September 6, 2016** for:

1. **CIP-003-7 - Cyber Security – Security Management Controls**
2. **CIP-003-7 implementation plan**
3. **The new term - Low Impact External Routable Communication (LERC) and its definition**

Commenting

Use the electronic form to submit comments. If you experience any difficulties using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

Join the Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Friday, August 19, 2016.** Registered Ballot Body members may join the ballot pools here.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 8 p.m. Eastern).

Next Steps

Initial ballots for the standard, implementation plan, and the new term for and definition of LERC, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **August 26 – September 6, 2016**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | CIP-003-7, Implementation Plan, and definiton of LERC
Comment Period Start Date:	7/25/2016
Comment Period End Date:	9/6/2016
Associated Ballots:	2016-02 Modifications to CIP Standards CIP-003-7 Implementation Plan IN 1 OT 2016-02 Modifications to CIP Standards CIP-003-7 IN 1 ST 2016-02 Modifications to CIP Standards CIP-003-7 Non-binding Poll IN 1 NB 2016-02 Modifications to CIP Standards Low Impact External Routable Communication | New Term/Definition IN 1 DEF

There were 81 sets of responses, including comments from approximately 76 different people from approximately 68 companies representing 9 of the Industry Segments as shown in the table on the following pages.

Questions

1. Definition: The SDT replaced the term *Low Impact External Routable Connectivity* with *Low Impact External Routable Communication (LERC)* and revised the definition such that it is relevant to the type of communication that occurs crossing the boundary of the BES asset that contains the low impact BES Cyber Systems. This more clearly aligns with the output of CIP-002-5.1 Requirement R1, Part 1.3. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

2. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 2 Physical Security Controls to reflect the retirement of LEAP. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

3. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 3 Electronic Access Controls to require entities to implement electronic access control(s) for LERC, if any, to permit only necessary electronic access to low impact BES Cyber System(s). Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

4. Measure M2: The SDT revised the complementary language of CIP-003-6, Attachment 2, Sections 2 and 3 to make the evidential language of the Measure consistent with the revised requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides example diagrams that illustrate various electronic access controls at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) for the revisions made to Sections 2 and 3 of Attachment 2 in CIP-003, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is nine (9) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If not, please provide the basis for your disagreement and an alternate proposal.

7. If you have additional comments on the proposed revisions to address the FERC directive regarding the LERC definition that you have not provided in response to the questions above, please provide them here.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Chris Gowder	Chris Gowder		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utility Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Stan Rzad	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steve Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Mark Brown	City of Winter Park	4	FRCC

					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	9	FRCC
Public Service Enterprise Group	Christy Koncz	1,3,5,6	NPCC,RF	PSEG	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	PSEG - Energy Resources and Trade LLC	6	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co.	1	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
SERC Reliability Corporation	David Greene	10	SERC	SERC CIPC	Bill Peterson	SERC RRO	10	SERC
					Mike Hagee	SERC RRO	10	SERC
					SERC CIPC	Various	1,2,5,9	SERC
MRO	Emily Rousseau	1,2,3,4,5,6	MRO	MRO-NERC Standards Review Forum (NSRF)	Joe Depoorter	Madison Gas & Electric	3,4,5,6	MRO
					Chuck Wicklund	Otter Tail Power Company	1,3,5	MRO
					Dave Rudolph	Basin Electric Power Cooperative	1,3,5,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Jodi Jenson	Western Area Power Administration	1,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Mahmood Safi	Omaha Public Utility District	1,3,5,6	MRO

					Shannon Weaver	Midwest ISO Inc.	2	MRO
					Mike Brytowski	Great River Energy	1,3,5,6	MRO
					Brad Perrett	Minnesota Power	1,5	MRO
					Scott Nickels	Rochester Public Utilities	4	MRO
					Terry Harbour	MidAmerican Energy Company	1,3,5,6	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,4,5,6	MRO
					Tony Eddleman	Nebraska Public Power District	1,3,5	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
Joe McClung	Joe McClung		FRCC	JEA Voters	Ted Hobson	JEA	1	FRCC
					Ted Hobson	JEA	1	FRCC
					Garry Baker	JEA	3	FRCC
					Garry Baker	JEA	3	FRCC
					John Babik	JEA	5	FRCC
					John Babik	JEA	5	FRCC
Con Ed - Consolidated Edison Co. of New York	Kelly Silver	1	NPCC	Con Edison	Kelly Silver	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange and Rockland Utilities	NA - Not Applicable	NPCC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation	6	SERC

						and Energy Marketing		
BC Hydro and Power Authority	Patricia Robertson	1		BC Hydro	Patricia Robertson	BC Hydro and Power Authority	1	WECC
					Venkataramakrishnan Vinnakota	BC Hydro and Power Authority	2	WECC
					Pat G. Harrington	BC Hydro and Power Authority	3	WECC
					Clement Ma	BC Hydro and Power Authority	5	WECC
Seattle City Light	Paul Haase	1,3,4,5,6	WECC	Seattle City Light	Pawel Krupa	Seattle City Light	1	WECC
					Dana Wheelock	Seattle City Light	3	WECC
					Hao Li	Seattle City Light	4	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Bud Freeman	Seattle City Light	6	WECC
					Paul Haase	Seattle City Light	1,3,4,5,6	WECC
					Ginette Lacasse	Seattle City Light	1,3,4,5,6	WECC
PPL - Louisville Gas and Electric Co.	Robert Tallman	3,5,6	RF,SERC	LG&E and KU Energy	Bob Tallman	LG&E and KU Energy	3,5,6	SERC
					Charlie Freibert	LG&E and KU Energy	3	SERC
					Dan Wilson	LG&E and KU Energy	5	SERC
					Linn Oelker	LG&E and KU Energy	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,10	NPCC	RSC no NextEra	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC

					Wayne Sipperly	New York Power Authority	4	NPCC
					David Ramkalawan	Ontario Power Generation	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					Brian Shanahan	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Kathleen M. Goodman	ISO-NE	2	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Sean Bodkin	Dominion	4	NPCC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE

					Ronald Bender	Nebraska Public Power District	1,3,5	SPP RE
					Tara Smith	Sunflower Electric	1	SPP RE
					Steven Keller	Southwest Power Pool Inc.	2	SPP RE
					Louis Guidry	Cleco	1,3,5,6	SPP RE
Santee Cooper	Shawn Abrams	1		Santee Cooper	Tom Abrams	Santee Cooper	1	SERC
					Rene' Free	Santee Cooper	1	SERC
					Chris Jimenez	Santee Cooper	1	SERC
					Troy Lee	Santee Cooper	1	SERC
					Bob Rhett	Santee Cooper	5	SERC
Oxy - Occidental Chemical	Venona Greaff	7		Oxy	Venona Greaff	Occidental Chemical Corporation	7	SERC
					Michelle D'Antuono	Ingleside Cogeneration LP.	5	Texas RE
ACES Power Marketing	Warren Cross	1,3,4,5	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Brazos Electric Power Cooperative, Inc.	BREC	1,5	Texas RE
					Old Dominion Electric Cooperative	ODEC	3,4	SERC
					Golden Spread Electric Cooperative	GSEC	5	SPP RE
					Prairie Power, Inc.	PPI	1,3	SERC
					Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF
					Buckeye Rural Electric Cooperative, Inc.	BUCK	4	RF
					Wabash Valley Power Association	WVPA	3	SERC

					East Kentucky Power Cooperative	EKPC	1,3	SERC
					Central Iowa Power Cooperative	CIPCO	1	MRO
					Rayburn Country Electric Cooperative, Inc.	RCEC	3	SPP RE

1. Definition: The SDT replaced the term *Low Impact External Routable Connectivity* with *Low Impact External Routable Communication (LERC)* and revised the definition such that it is relevant to the type of communication that occurs crossing the boundary of the BES asset that contains the low impact BES Cyber Systems. This more clearly aligns with the output of CIP-002-5.1 Requirement R1, Part 1.3. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6

Answer	No
Document Name	

Comment

: What is the “Bounder of the BES asset”? I believe this should say “crossing the defind boundery of the BES asset” The word "asset" is also a problem I think it is to broad. I am not sure how to narrow the focus.

Likes 1	Michael Watkins, N/A, Watkins Michael
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

he definition contains two terms that we respectfully suggest should be defined terms as they are fundamental to the meaning of LERC and subsequently critical to meeting compliance requirements of any standards/requirements that use the term.

"BES asset boundary" is used in numerous instances within the standard attachments and it is assumed that it is synonymous with the term "boundary of an asset", which is used in the definition of LERC. What is meant by the term is described in the GTB, "Requirement R2, Attachment 1, Section 3 - Electronic Access Controls". Because there is no correlation between the GTB of the standard and the LERC definition there is no way to understand the term "boundary of an Asset" when reading the LERC definition. The concept of the asset boundary as used in the LERC definition is critical to the meaning of the term LERC and as such it is critical that it be clear and unambiguous. The only way to do that is through the use of a define term or define it within the LERC definition.

"intelligent electronic devices" is used in the definition and in several instances within the GTB of the standard but it is not a common term to the extent that it is unambiguous. We respectfully suggest that the term should be clearly defined as a defined term. The word "intelligent" within the term is very subjective and can be interpreted in many different ways. For example it could be interpreted to mean "artificial intelligence" or it could be interpreted to mean "can perform an action without specific direction". "artificial intelligence implies a very sophisticated level of computing where "can perform an action without specific direction" could be a simple timer.

As both of these terms are paramount to the understanding of the term LERC we suggest that they be appropriatly included as a defined term or defined within the LERC definition.

Likes 0	

Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	No
Document Name	

Comment
The proposed definition raises more ambiguity than the current definition and goes beyond the direction of the FERC order. The definition needs to clearly state whether outbound and inbound communications are being considered and use terminology and structure similar to what is used for other protected measures. Further, physical and electronic characteristics are confused.

Likes 0	
Dislikes 0	

Response

Emily Rousseau - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)	
Answer	No
Document Name	

Comment
The change in definition of LERC will require more documentation about each low impact asset's external communication than what is required for medium impact assets. We would prefer the current definition of LERC (Low Impact External Routable Connectivity) versus the proposed definition. It does not require documentation of electronic access controls if there is no routable connection to low impact BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment
The definition needs clarification as it is vague. It may be necessary to carefully identify inclusions and exclusions (similar to the BES definition). If both are defined, clear identify priority among the inclusions and exclusions. Please note that the term LERC is improperly used throughout the Guidelines and Technical Basis by referring to communications not involving any low impact BES Cyber System as LERC.

The definition includes any routable communication that crosses a BES asset boundary. This definition would encourage adding new requirements for BES assets containing only low impact BES Cyber Assets regulating communication paths into a site unrelated to the BES. For example, if a corporate network is present for local use such as for a maintenance work order system is present, then the low impact BES Cyber Assets are now subject to the requirements of the Standard. As written, even a person walking inside a BES asset boundary with a smartphone having web access would elevate the site to having LERC as the phone utilizes IP. This definition is unworkable.

In practice, the inconsistency between the definition and attachment 1 section 3 potentially adds to confusion on the initial reading of the requirements. Further, the need for 9 example models and 12 pages in the Guidelines and Technical Basis to explain the definition indicates there is a fundamental problem with the approach.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

1. Regarding the shift to the asset physical boundary for determination of whether LERC exists at the asset:

All the examples provided in the Guidelines and Technical Basis are physical boundaries, such as property or fence lines. Shifting the point of demarcation for LERC to the BES asset physical boundary such as property or fence lines pushes LERC far away in proximity from the BCSs. The resulting shift in focus to LERC will make controlling BCS electronic access more difficult.

In addition, placing LERC at the physical asset boundary means the corresponding infrastructure will likely be maintained by groups who do not currently have the responsibility for electronic access controls for the BCS.

For example: Temporary office trailers are frequently brought onsite to house the additional staff to support large projects. No matter how they are connected, it will be far removed from any BCS impact, but if it crosses the BES asset boundary, it appears LERC would have to be identified and assessed.

The entity suggests the drafting team revise the language to clarify that an inventory or assessment of communications paths to the asset is not required for assets the entity has determined to have LERC.

2. Regarding controls for “Cyber Asset(s) that provide electronic access”:

The Guidelines and Technical Basis states that the “BES asset boundary” is synonymous to the concept of a “logical border” demarcation.

Does the responsible entity have the option to declare the BES asset boundary “closer in” to the BCSs than a perimeter fence, such as declaring a logical border around the asset’s control network, which includes all BCSs, and excludes many non-essential networks, such as an IT owned and operated business network?

The entity suggests the drafting team revise the language to clarify that the entity has the responsibility for determining the appropriate location within the logical infrastructure to implement electronic access controls required by Attachment 1 Section 3.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	No
Document Name	
Comment	

Seattle appreciates the efforts the Standards Drafting team to address FERC's questions about LERC as expressed in Order 822 but does not agree with the proposed approach.

Modification to LERC definition draws into scope routable communications among non-BES Cyber Systems isolated from BES Cyber Systems or BCS communication networks. For example, as written, LERC would apply to a business network-connected desktop computer at a Low impact location--that by itself is not and has no connection to any BES Cyber System--solely because the routable communications from the non-BES system cross the boundary of the Low impact site. As such, a Low impact asset with BES Cyber Systems that lack any routable connectivity would still have LERC (and thus require the protections of CIP-003-7) if there was a routable business network—or any other routable communications, even presumably a hotspot enabled by a cellphone located outside the asset (site)—present.

This change greatly expands the scope of LERC under the proposed definition. Indeed, in a very real sense, it makes it all but impossible for a low impact asset (site) not to have LERC. This change goes far beyond the request of FERC in Order 822 to address what is meant by “directly” connected and is not warranted nor necessary.

As a possible corrective that restores the scope of LERC to something similar to the present scope, Seattle City Light suggests additional language for the definition of LERC such as “Routable protocol communication AMONG ONE OR MORE BES CYBER SYSTEM(S) that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), excluding…” (CAPITALS indicate additions).

Also, please clarify if LERC is intended to apply to an entire asset (site) or if on a system-by-system basis. The previous definition of LERC clearly applied to individual BES Cyber Systems, in that one BCS at an asset might have LERC and another at the same asset might not have LERC. The new definition, as written, appears to define LERC as a characteristic of the asset (site) as opposed to a characteristic of a cyber system or a BES Cyber System. Seattle City Light recommends clearly stating whichever approach in intended, and strongly prefers language to retain the existing system-based approach. As such, Seattle recommends adding the following sentence at the end to the LERC definition: “THE PRESENCE OR LACK OF LERC IS EVALUATED INDIVIDUALLY FOR EACH BES CYBER SYSTEM EXISTING AT AN ASSET.”

Finally the “Determining Asset Boundary” discussion in the CIP-003-7 Supplemental Material should be revised to clearly state that 1) routable communications on business networks and other non-BES networks having no connection to BES Cyber Systems are excluded from LERC, and that 2) LERC is a property of individual BES Cyber Systems and not a property of an asset (site) as a whole.

Likes 1	Black Hills Corporation, 1, Wingen Wes
Dislikes 0	

Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	No
Document Name	
Comment	

We recommend replacing “communication” with “connectivity” because communication may weaken the security of the cyber asset. Securing connectivity protects against all attacks using that network pathway. Only securing against communications path would allow reduced security. Because you can be connected without communicating per the OSI layers. Connectivity and communications are diferent OSI layer, which opens up the possibility of connectivity without communications. This leaves a path for attackers to connect through the asset’s boundary.

Previous definition was more clear and resulted in less burden on Registered Entities. The propsed definition adds administrative burden without adding any reliability benefit to the BES. Additionally designating an entire asset as LERC may rope non-BES Cyber Assets into compliance with potential future Standards aimed at protecting LERC assets.

If proposed definition must stay:

Physical demarcation (asset boundary) for logical controls does not make sense. As written it is too prescriptive; owners should be allowed discretion on boundary. We propose to allow Entities to define their own logical boundary or boundaries within a low impact asset, essentially a low impact ESP (LESP). An LESP would allow an entity the ability to narrow the scope of applied controls and regulation to low impact Cyber Systems, as CIP is intended, without involving systems that have no reliability impact. Additionally an entity that only has many Low Impact Systems would still have the ability to label the whole site as an LESP or Low Impact Security Zone (LISZ). The LESP would not carry over typical requirements of ESPs so use of the term LISZ may avoid confusion.

Alternatively, we suggest adding a clause to the definition such that the cross boundary communication must be associated with the functionality or operability of the low impact Cyber Systems to constitute LERC. This eliminates the issues below that arise with the current proposed definition:

- Wireless communications, which have no impact on low impact BCS (data enabled cell phone), create the existence of temporary LERC. Given the prevalence of mobile phones, it is hard to imagine a substation which does not have LERC at some time.
- Air gapped configurations do not have the same risk profile as networked substations, but both will be labeled as LERC, thereby undermining the signaling impact of a LERC label. It also creates administrative burden with no reliability impact.
- Certain assets which contain low and medium impact BCS may be listed as non-ERC and LERC. This is unnecessarily confusing.

Remove phrase “or vendor proprietary protocol”. This incentives entities to adopt vendor proprietary protocols to avoid compliance obligation. Incentivizing diverse protocols will reduce the ability of entities to use compatible devices for security solutions in the future.

Likes 1	New York State Reliability Council, 10, ADAMSON ALAN
Dislikes 0	

Response

Erika Doot - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Reclamation is concerned that the proposed LERC definition would encompass corporate network or personal devices that do not monitor or control BES assets, and have no connectivity to BES assets. Reclamation does not believe that all routable devices within the perimeter of BES assets should fall within the scope of CIP standards. Indeed, In the red-line draft for CIP-003-7, the revised standard often uses the term "Cyber Asset" instead of

BES Cyber Asset" which can be an indication that the scope was inadvertently expanded. Reclamation requests that the proposed LERC definition be restricted to include only routable devices which monitor or control BES assets, and which would impact the BES if damaged or compromised.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Alternatively, we suggest adding a clause to the definition such that the cross boundary communication must be associated with the functionality or operability of the low impact Cyber Systems to constitute LERC. This eliminates the issues below that arise with the current proposed definition:

- *Wireless communications, which have no impact on low impact BCS (data enabled cell phone), create the existence of temporary LERC. Given the prevalence of mobile phones, it is hard to imagine a substation which does not have LERC at some time.*
- *Air gapped configurations do not have the same risk profile as networked substations, but both will be labeled as LERC, thereby undermining the signaling impact of a LERC label. It also creates administrative burden with no reliability impact.*

Likes 1	New York State Reliability Council, 10, ADAMSON ALAN
Dislikes 0	

Response

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

I. A primary concern is that the new definition applies to routable communications at a facility that leave that facility (“boundary of the asset”). This is a change from the previous use and definition of LERC, as LERC was previously applied to communications between BES Cyber Assets. This requires the registered entity to focus compliance gathering efforts on non-BES cyber assets with no routable connectivity to BES cyber assets. It is not clear whether this change was intended to include non-BES cyber assets as part of LERC.

II. Another concern is the phrase “time-control functions between non-Control Center BES assets,” the explicit inclusion of “non-Control Center BES assets” does not seem to add any value. There may be cases where time-sensitive protection functions exist between non-Control Center BES assets and Control Center assets.

III. The new definition needs to clarify how the term ‘asset’ is applied, since an asset as stated in CIP-002-5.1, R1.i through R1.vi can mean facilities, components, or systems.

Proposed definition is as follows:

"Routable protocol communication that crosses the boundary of an asset, such as control center, substation, or generating station, containing external routable communications between one or more low impact BES Cyber System(s), excluding communications between intelligent electronic devices used for time mandatory protection or control GOOSE or vendor proprietary protocols."

Likes 0	
Dislikes 0	

Response

Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy

Answer	No
Document Name	

Comment

LG&E/KU's concern is based on adding the concept and/or definition of "boundary of an asset" to the LERC definition. While this appears to be more a "PSP-like" definition, LG&E/KU prefer the "demarcation" concept NERC presented in previous lessons learned and FAQs. The draft definition could make it difficult for the Responsible Entities to determine the exact boundary and when doing so, may introduce burdens the SDT is trying to eliminate, due to risk, with Low Impact systems. LG&E/KU understands the SDT desire to keep the "no inventory needed for Low" concept in place however, the administrative burden in the end may be the same. Since most of the facilities (generation plants for example) contain both control LANs and corporate LANs, it will now be necessary to produce both control LAN networks drawings along with corporate LAN network drawings in order to prove the "air gap", where before all that was required were the control LAN documentation. The final concern LG&E/KU has deals with the backhaul networks. In many cases the control LAN and other communication (data, voice, etc.) may be combined by a multiplexer to allow time sequenced priority over a single T1 line. In these cases, the multiplexer just passes the data to the next multiplexer in line and the T1 line could carry both routable and non-routable traffic, thus causing confusion over how to exactly classify this device.

LG&E/KU support most of the EEI comments on this requirement change, however, LG&E/KU would like to see the exemption from 4.2.3.2 included within the definition. NERC had endorsed the concept of creating a "demarcation point" at the Low Impact system to exclude those cyber assets within the communcation network. LG&E/KU suggests the LERC definition be:

"Any electronic routable protocol communcation entering or leaving the BES asset boundary that provides connectivity to Low Impact BES Cyber System(s), excluding communication between: (1) Low Impact BCS located at the same BES asset; (2) Cyber Assets associated with communication networks and data communication links between different BES assets boundaries and/or Electronic Security Perimeters; and (3) intelligent electronic devices used for time Exempt Cyber Systems mandatory protection or control including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols."

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No

Document Name	

Comment

The proposed revisions to the Low Impact External Routable Connectivity (LERC) definition, retirement of the Low Impact Electronic Access Point (LEAP) and associated changes to the requirements for CIP-003 Attachment 1 Section 2 and 3 represent a significant shift from the currently FERC-approved definitions and requirements. The proposed changes include identifying LERC to non-BES Cyber Assets increasing the scope. Entities are well into their implementation of the approved definitions and requirements. This fundamental shift creates regulatory uncertainty for entities and timing concerns to meet the proposed implementation schedule due to re-work and the volume of assets containing low impact BES Cyber Systems. At best, FERC approval is not likely till near the end of 2017, which will be too late for most entities' budgeting schedules for work to be completed in 2018 if the revised requirements require budget changes. It's not logical to vote yes on the non-binding poll until the requirement language is closer.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1,3, Gresham Darnez
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

We suggest the language: Communication that uses a routable protocol that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), excluding communications between intelligent electronic devices used for time [illegible] non [illegible] Control Center BES assets containing low impact BES Cyber Systems (i.e. IEC 61850 GOOSE or vendor proprietary protocols). We suggest the language: Communication that uses a routable protocol that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), excluding communications between intelligent electronic devices used for time [illegible] Control Center BES assets containing low impact BES Cyber Systems (i.e. IEC 61850 GOOSE or vendor proprietary protocols).

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

The terms associated with low impact electronic access controls should be congruent with the terms for medium and high impact. CenterPoint Energy believes the use of "ERC" should remain External Routable Connectivity. CenterPoint Energy recommends "LERC" to stand for "Low Impact External Routable **Connectivity**" with the following definition:

“The ability to access a low impact BES Cyber System from a Cyber Asset that is outside of its associated BES asset as identified in CIP-002 via a bi-directional routable protocol connection.”

Making this change should address the Commission’s directive as it gets rid of the term “direct” and aligns with the commentary in the Guidelines and Technical Basis section of CIP-003-6. Clarity is provided as this is the same term/concept that has been applied in medium and high impact facilities. It should be a matter of extending this concept to low impact facilities and implementing requirements at an appropriate level based on risk, low.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6

Answer	No
Document Name	

Comment

Considering the new NERC definition of LERC as “routable communication that crosses the boundary of an asset” in conjunction with Attachment 1 Section 3 Part 3.1 requiring the implementation of “electronic access control(s) for LERC”, these changes could be misinterpreted to mean that access controls are to be performed *at the boundary* of a BES asset since that is a key component of the definition of LERC. It is requested that the SDT add explicit language to the requirement or the Supplemental Material that reduces this risk of misinterpretation, such as, “…although LERC is contingent upon the routable communications crossing the BES Asset boundary, the controls to restrict access for Low Impact BCS with LERC are not required to be implemented at the BES Asset boundary, but instead in a manner that ensures that Applicable Systems are compliant with the control.” Without this explicit language, some entities may interpret the controls as being required at the BES Asset boundary. The existing language may inadvertently increase the scope of assets to include certain devices (i.e. those on the corporate network) that would normally be considered out-of-scope.

Likes 0	
Dislikes 0	

Response

Oliver Burke - Entergy - Entergy Services, Inc. - 1

Answer	No
Document Name	

Comment

I support comments submitted by Entergy's Julie Hall.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE appreciates the SDT's efforts to develop a workable response to FERC's directive in Order No. 822 to provide clarity and eliminate the ambiguity surrounding the term "direct" as it is used in the current definition of Low Impact Routable Connectivity. However, Texas RE is concerned that the SDT's proposed approach to resolving this ambiguity by shifting the focus away from connectivity to communications across an asset boundary is not workable. Moreover, the proposed revisions introduce a number of new terms and concepts that, absent clarification, could result in additional confusion across the industry. Instead, Texas RE recommends that the SDT address FERC's directive by eliminating the distinction between "direct" language from the definition of LERC and adopt familiar concepts from the general definition of External Routable Connectivity (ERC) to the Low Impact Cyber Asset environment.

Texas RE is concerned the proposed LERC definition could be read to exclude serial data communications across an asset boundary. Such serial communications may not be exclusively serial in nature because the serial data could be encapsulated and decapsulated (TCP/IP). As such, the data flow still constitutes bi-directional routable protocol that is within the scope of the general ERC definition. Similarly, Texas RE believes that the LERC definition should capture all bi-directional routable protocols, including serial communications that have been converted to use TCP/IP protocols. This is particularly important for reliability because, in Texas RE's experience, significant amounts of data from relays and RTUs (among other devices) are communicated in this fashion.

Conversely, it is possible to interpret the proposed LERC definition as a significant expansion of the current CIP requirements. In particular, because the proposed definition now focuses on "communications" across an asset boundary, a host of communications could now establish the basis for LERC. For example, a cell phone may pass communication data across an asset boundary, potentially making such devices subject to CIP requirements including electronic access controls.

Finally, the proposed LERC definition introduces a number of new or undefined terms that could cause confusion. Specifically, the proposed definition and supporting attachments use terms such as "assets", "BES asset(s)", "non-Control Center BES assets", "non -BE Boundary" in a potentially confusing manner, particularly in connection with uses in other CIP Standards. For example, CIP-002-5.1, R1 uses the term "assets" where CIP-003-7 uses the term "assets" and "BES asset(s)". Another example, Attachment 1 and 2, both use the term "asset(s)."

In light of these concerns, Texas RE respectfully suggests that the SDT modify its approach to addressing the FERC directive. Specifically, rather than introducing new concepts into the LERC definition, the SDT could address FERC's concerns regarding the use of the term "direct" by eliminating that concept from the LERC definition and instead revising the LERC definition along the lines of the current ERC definition. The ERC is currently defined as: "[t]he ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection." At present, Low Impact BES Cyber Systems currently do not have associated Electronic Security Perimeters. The SDT may wish to consider extending the Electronic Security Perimeter requirement to Low Impact BES Cyber Systems as well. Short of this, however, the SDT should revise the LERC definition to track the ERC definition, but eliminate the ESP concept. For example, LERC could be defined as "[t]he ability to access a BES Cyber Systems from a Cyber Asset that is outside of BES Cyber System's asset boundary via a bi-directional routable protocol connection."

Additionally, Texas RE suggests, under R2, the language that reads "*Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required*"; should be removed. Texas RE considers keeping a list of BES Cyber Assets as best practice and the note discourages it. Texas RE encourages entities to have an inventory of their low impact BES Cyber Systems. This type of evidence would line up properly with Attachment 2 and the Guidelines and Technical Basis for Sections 2 and 3. It does not make good business sense to not have a list associated with an asset inventory. There is not a business manager who would encourage not knowing the level of effort needed to perform a job function and the job function here is reliability. Not having a list is going to extend the amount of effort during an audit for the registered entity and the regional entity staff. This attempt to lower compliance risk is detrimental to reliability. If a company does not maintain an inventory how can it be successful in ensuring that efforts to maintain security of that inventory are complete?

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	

Comment

The change of the definition of LERC to any routable communication that crosses the "BES asset" boundary containing Low Impact BES Cyber Systems will create LERC even where there is no communication with BES Cyber Assets. While this *may* reduce confusion over where there is LERC, it significantly increases the documentation necessary to ensure proper access controls (Physical or Logical Isolation) for netowkrs that have no relation to BES control functionality.

Better would be to limit LERC to the affirmative in relation to communication with a BES Cyber System.

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	

Comment

The term "boundary of an asset" used in the definition needs to be better defined as opposed to leaving the interpretation up to the reader. The guidance in the Standard itself offers reasonable suggestions that all appear to extend no further than the physical property boundary of the asset. However, guidance is not binding and left to devise an asset boundary of its own choosing, a Registered Entity potentially could create an unreasonable boundary. The SPP RE suggests that "boundary of an asset" be replaced with "property or fence line of an asset". Alternatively, the definition could incorporate the physical access control boundary as established by Section 2 of Attachment 1 to CIP-003-7 such that any traffic crossing that perimeter would be considered LERC.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

The LERC definition coupled with the CIP-003-7 R2, Attachment 1, Section 3 creates administrative burdens that encourage Responsible Entities and auditors to focus their efforts on compliance evidence for assets that have no connectivity to low impact BES Cyber Systems (“LIBCS”). Understandably, the SDT is looking to address the FERC directive to eliminate the ambiguity caused by the term direct in the LERC definition, while trying to avoid requiring Responsible Entities to list LIBCS. While LERC now has more clarity, it is defined in broader terms that will require more evidence to prove that LIBCS do not communicate over LERC, which could be a substantial burden for entities with large numbers of assets.

The use of “boundary of an asset” is similar to the high and medium impact BES Cyber Systems (“BCS”) ESP concept, which creates similar compliance burdens. The risk-based approach of the CIP Standards is meant to focus security and compliance efforts on the most critical assets, the high and medium impact BCS. Applying a similar concept to the LIBCS may dissolve this risk-based approach and encourages auditors to require lists of LIBCS. However, given diversity among Responsible Entity assets, systems, and security approaches, we think it is important to focus on the security objective.

The security objective is to control electronic access to LIBCS such that only necessary and authorized electronic access is allowed. Proving that this security objective is met can be accomplished in multiple ways and at the site, network, or LIBCS level. For example, here are two approaches:

1) Analyze all external connectivity to the asset to see if there is LERC. If a connectivity path meets the LERC definition, implement and document the electronic access control(s) used to “permit only necessary electronic access” to any LIBCS that may reside within the asset.

2) Analyze all LIBCS or their networks and then implement and document the electronic access control(s) and prove the external connectivity/dial-up to all of them.

For some low impact assets, especially large assets with thousands of LIBCS, the first approach may be more feasible. For others with large numbers of low impact assets, especially those with a higher amount of LERC that does not connect to LIBCS, the second approach may be more feasible. The standard should allow flexibility for entities to use these or other methods for documenting LERC in a way that reduces the documentation burden.

To address these issues as well as the implementation issues mentioned under question 6, EEI encourages the SDT to adopt an approach that allows for both methods. One approach to consider, in addition to removal of LEAP, is also removing the LERC definition and focusing on the security objective in Attachment 1, Section 3. We propose alternative language in our answer to question 3.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Jeffrey Watkins - Jeffrey Watkins On Behalf of: Eric Schwarzrock, Berkshire Hathaway - NV Energy, 5; - Jeffrey Watkins

Answer	No

Document Name	

Comment

NV Energy has concens with the proposed definition change. The proposed changes include identifying LERC to non-BES Cyber Assets increasing the scope. The change in definition of LERC will require more documentation about each low impact asset's external communication than what is required for medium impact assets. This change in scope could potentially be burdensome especially since some entities are well into their implementation of the approved definitions and requirements.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no NextEra

Answer	No
Document Name	

Comment

We recommend replacing "communication" with "connectivity" because communication may weken the security of the cyber asset. Securing connectivity protects against all attacks using that network pathway. Only securing against communications path would allow reduced security. Because you can be connected without communicating per the OSI layers. Connectivity and communications are diferent OSI layer, which opens up the possibility of connectivity without communications. This leaves a path for attackers to connect through the asset's boundary. Otherwise, we agree with the new definition.

The definition contains two terms that we suggest should be defined terms as they are fundamental to the meaning of LERC and subsequently critical to meeting compliance requirements of any standards/requirements that use the term.

"BES asset boundary" is used in numerous instances within the standard attachments and it is assumed that it is synonymous with the term "boundary of an asset", which is used in the definition of LERC. What is meant by the term is described in the Guidelines and Technical Basis, "Requirement R2, Attachment 1, Section 3 - Electronic Access Controls". Because there is no correlation between the Guidelines and Technical Basis of the standard and the LERC definition there is no way to understand the term "boundary of an Asset" when reading the LERC definition. The concept of the asset boundary as used in the LERC definition is critical to the meaning of the term LERC and as such it is critical that it be clear and unambiguous. The only way to do that is through the use of a define term or define it within the LERC definition.

"intelligent electronic devices" is used in the definition and in several instances within the Guidelines and Technical Basis of the standard but it is not a common term to the extent that it is unambiguous. We suggest that the term should be clearly defined as a defined term. The word "intelligent" within the term is very subjective and can be interpreted in many different ways. For example it could be interpreted to mean "artificial intelligence" or it could be interpreted to mean "can perform an action without specific direction". "artificial intelligence implies a very sophisticated level of computing where "can perform an action without specific direction" could be a simple timer.

As both of these terms are paramount to the understanding of the term LERC we suggest that they be appropriatly included as a defined term or defined within the LERC definition.

Previous definition was more clear and resulted in less burden on Registered Entities. The propsed definition adds administrative burden without adding any reliability benefit to the BES. Additionally designating an entire asset as LERC may rope non-BES Cyber Assets into compliance with potential future Standards aimed at protecting LERC assets.

If proposed definition must stay:

Physical demarcation (asset boundary) for logical controls does not make sense. As written it is too prescriptive; owners should be allowed discretion on boundary. We propose to allow Entities to define their own logical boundary or boundaries within a low impact asset, essentially a low impact ESP (LESP). An LESP would allow an entity the ability to narrow the scope of applied controls and regulation to low impact Cyber Systems, as CIP is intended, without involving systems that have no reliability impact. Additionally an entity that only has many Low Impact Systems would still have the ability to label the whole site as an LESP or Low Impact Security Zone (LISZ). The LESP would not carry over typical requirements of ESPs so use of the term LISZ may avoid confusion.

Alternatively, we suggest adding a clause to the definition such that the cross boundary communication must be associated with the functionality or operability of the low impact Cyber Systems to constitute LERC. This eliminates the issues below that arise with the current proposed definition:

· Wireless communications, which have no impact on low impact BCS (data enabled cell phone), create the existence of temporary LERC. Given the prevalence of mobile phones, it is hard to imagine a substation which does not have LERC at some time.

· Air gapped configurations do not have the same risk profile as networked substations, but both will be labeled as LERC, thereby undermining the signaling impact of a LERC label. It also creates administrative burden with no reliability impact.

· Certain assets which contain low and medium impact BCS may be listed as non-ERC and LERC. This is unnecessarily confusing.

Remove phrase “or vendor proprietary protocol”. This incentives entities to adopt vendor proprietary protocols to avoid compliance obligation. Incentivizing diverse protocols will reduce the ability of entities to use compatible devices for security solutions in the future.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 5

Answer	No
Document Name	

Comment

AZPS interprets the proposed revisions to the term *Low Impact External Routable Connectivity* to *Low Impact External Routable Communication* (LERC); such that LERC would be relevant to communication that occurs at the boundary of a BES asset that contains low impact BES Cyber Systems (BCS), rather than at the boundary of the BCS, and, therefore, would encompass all cyber assets within that boundary. As such, AZPS is opposed to requiring LERC at the boundary of a BES asset as it will not only significantly increase the scope of this requirement by encompassing assets that are not identified as BCS, but will also increase the complexity of operational functionality and introduce unnecessary risk to the Bulk Electric System (BES) by not having controls that are localized and focused on the BCS.

Likes 0	

Dislikes 0	

Response

Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG

Answer	No
Document Name	

Comment

PSEG agrees with and supports EEI's comments.

Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

Please consider eliminating LERC as a defined term. The definition of LERC is too broad and will cause confusion regarding the concept of asset “boundary”. In addition, the exclusion of “communication protocols for time-sensitive protection or control functions” presents a reliability risk. Rather than “future-proofing” the requirement, this exclusion permits future cyber security risks for time-sensitive communications. Effective implementation of time-sensitive communications needs some level of security measures in order to ensure reliable real-time communications. At the same time, the Standard should avoid prescribing what electronic access controls are required for time-sensitive communications. The Responsible Entity should have the latitude to decide what protections are necessary based on engineering requirements. The discussion of time-sensitive communications and vendor proprietary protocols should not be part of a defined term and should be moved to Attachment One Section 3 (if the exclusion must be kept) or to the Guidelines.

Attachment 2 Section 3.1 can be written without referring to “LERC”. Please see suggested language in comment for CIP-003-7.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

The new definition causes confusion in that it requires a separate and different process than is required for Medium Impact assets. Consider the process to update documentation for a low impact asset that grows to a medium. Now a completely separate process must be initiated to provide medium impact compliant documentation.

Equally as important, this change will require the inclusion of any BES asset which has a completely isolated and self-contained, non-connected, BES Cyber System and a completely separate administrative or security network. There is no security benefit to be gained and compliance would require a tremendous effort by industry. Some companies may even consider removing IP based administrative or security systems to avoid the compliance burden if there is no other IP connection at particular substations.

The change in definition of LERC will require a great deal of work to research and document. It will probably require even more man hours than what is required for medium impact assets. That documentation doesn't compile itself. It takes engineers and technicians making trips to every asset to document what is there.

We would prefer the current definition of LERC (Low Impact External Routable Connectivity) versus the proposed definition. It does not require documentation of electronic access controls if there is no routable connection to low impact BES Cyber Assets.

We went through a great deal of confusion to finally have a common understanding of External Routable Connectivity, introducing a new term will very likely lead us all through that painful process yet again.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

The new definition causes confusion in that it requires a separate and different process than is required for Medium Impact assets. Consider the process to update documentation for a low impact asset that grows to a medium. Now a completely separate process must be initiated to provide medium impact compliant documentation.

Equally as important, this change will require the inclusion of any BES asset which has a completely isolated and self-contained, non-connected, BES Cyber System and a completely separate administrative or security network. There is no security benefit to be gained and compliance would require a tremendous effort by industry. Some companies may even consider removing IP based administrative or security systems to avoid the compliance burden if there is no other IP connection at particular substations.

The change in definition of LERC will require a great deal of work to research and document. It will probably require even more man hours than what is required for medium impact assets. That documentation doesn't compile itself. It takes engineers and technicians making trips to every asset to document what is there.

We would prefer the current definition of LERC (Low Impact External Routable Connectivity) versus the proposed definition. It does not require documentation of electronic access controls if there is no routable connection to low impact BES Cyber Assets.

We went through a great deal of confusion to finally have a common understanding of External Routable Connectivity, introducing a new term will very likely lead us all through that painful process yet again.

Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	No
Document Name	
Comment	
The proposed revised LERC definition expands the scope for evidence requirements to include connectivity to non-BES Cyber Assets. For example, an entity may not have LERC to the BES Cyber Assets at an asset, but may have LERC to non-BES Cyber Assets. The change in the definition requires entities to identify LERC to non-BES Cyber Assets then provide evidence that this new LERC does not connect to BES Cyber Assets. The scope change creates regulatory uncertainty and issues with completing new work within the proposed implementation schedule. The alternate proposal to retire the LERC definition addresses the FERC directive to address ambiguity of “direct.” The alternate proposal for Attachment 1 Section 3, in response to question 3, captures the obligation for the Responsible Entity. Alternate proposal: Retire the LERC definition, see alternate proposal for question 3.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy supports the comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	

Hydro One supports comments submitted by NPCC RSC.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment

The proposed definition as written would allow for the introduction of devices such as smart phones, laptops, tablets, or other devices that if they had connection to a wireless network or some other type of routable connection would be considered LERC and be subject to the applicable sections of CIP-003-7.

The definition does not adequately distinguish between BES Cyber Assets and non-BES Cyber Assets. An added 'bright line' must be included so low impact BES Cyber Systems that have no association, connection or ability to communicate with non-BES Cyber Assets don't drag a "BES asset" into having LERC. For example, with the current definition, a person carrying a smartphone inside the "asset boundary" could create LERC, even though there may be no way for that device to communicate with the BES Cyber Asset. The definition of LERC must include the requirement that the communication pass through an electronic access control device before being permitted to or from the BES Cyber System.

That will result in additional documentation for entities to document those devices that have LERC but are not connected to any BES Cyber System.

Further, the need for 9 example models and 12 pages in the Guidelines and Technical Basis to explain the definition indicates there is a fundamental problem with the approach.

Likes 0	
Dislikes 0	

Response

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No
Document Name	

Comment

JEA supports the LPPC comments.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

By removing the term "bi directional routable protocol access" from Attachment 1, the SDT has inadvertently caused further vagueness about what protocols are to be included within the requirement. As written this would allow for introduction of devices such as smart phones, laptops, tablets, or other devices that have a connection to a wireless network or some other type of routable connection could be considered LERC and be subject to CIP-003-7.

We propose to modify the definition of LERC to be "Routable protocol communications that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), excluding communications between equipment outside of the site communications demarcation point, or communications between intelligent electronic devices used for time-sensitive protection or control functions between non-Control Center BES assets containing low impact BES Cyber Systems including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols." Additionally, we suggest modifying R3.1, Section 3, Attachment 1 to be "Implement electronic access control(s) for LERC, if any, to permit only necessary bi directional routable protocol access to low impact BEC Cyber System(s)."; and modify the Guidelines and Technical Basis section Determining LERC, Requirement R2, Attachment 1, Section 3 - Electronic Access Controls.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

In our observation, we noticed that the SDT mentions in its background information the changes to the components of the term ‘LERC’. Additionally, the revision to the definition to provide more clarity for the term (in a different documentation). Also, we’ve observed the term and reference of its definition in the Supplement Guidance Section of the Standard. With that being said, we would suggest to the drafting team to include a section at the beginning of the Standard labed **New or modified Term(s) used in NERC Standards.** This will help the drafting team keep the industry up to date on what new terms have been added or revised in a particular Standard as well as promoting consistency with the formatting of the Standards Development Process.

As for the revision to the definition, we would ask the drafting team does clarity need to be provided on what an ‘intelligent electronic system’ is? Not to be difficult…but aren’t all electronic devices intelligent???. Maybe, the drafting can provide some clarity on that process. Additionally, we would ask that the draft team would they provide clarity on the term ‘boundary’ in the definition to align to the contentds as it states in the guidance documentation.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA supports the comments of American Public Power Association.

Likes 0	
Dislikes 0	

Response

Jay Barnett - Exxon Mobil - 7

Answer	No
Document Name	

Comment

Although I agree with the flexibility added to the CIP-003, I believe the proposed modification to the definition LERC is too broad. The concern is that entities and auditors could differ on which communications are LERC depending on how they define the boundary of the asset. LERC should be defined such that equipment that doesn't communicate with or impact a BES Cyber Asset is not included within the scope of CIP-003.

Likes 0	
Dislikes 0	

Response

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No

Document Name	
Comment	
JEA supports the LPPC comments.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST recommends that at a minimum, the definition be revised to clarify what is meant by the “boundary” of an asset. The “CIP-003-7 Supplemental Material” section of CIP-003-7 Draft 1 includes a helpful discussion of the topic (“Determining Asset Boundary”), but N&ST notes that almost since the first version of the CIP Standards became mandatory and enforceable, Responsible Entities have vigorously opposed the so-called practice of “auditing to guidelines.” Absent a clear description of what is meant by “boundary,” the proposed definition of LERC is ambiguous. N&ST recommends that the SDT consider incorporating the draft guideline statement, “The intent is for the Responsible Entity to define the BES asset boundary such that the low impact BES Cyber System(s) that are located at the BES asset are contained within the BES asset boundary,” into the LERC definition.

A second problem with the proposed definition is the fact that, in combination with the proposed revisions to CIP-003-6, it would bring low impact BES Cyber Systems with no network connectivity at all into scope for the requirement to “Implement electronic access controls” (CIP-003-7 Draft 1, Attachment 1, Section 3, Part 3.1) if the BES asset happened to also contain non-BES Cyber Assets with routable connectivity to and from other sites (a corporate network PC, for example). N&ST is certain that entities would prefer to not experience a repeat of the problems caused by the wording of CIP Versions 1-3, which stated entities must have procedures for securing dial-up access to Electronic Security Perimeters and made no allowances for situations where no dial-up access existed. An entity should be required to identify and document that LERC exists at a given BES asset only if one or more low impact BES Cyber Systems at that asset have routable connectivity to and from other sites. The exception for direct, time-sensitive communication between IEDs and similar devices should be maintained.

Finally, N&ST believes that the SDT’s decision to address the problem of what is meant by “direct” communication with low impact BES Cyber Systems by eliminating the word from the definition will fail to put the matter to rest. “LERC Reference Model 4” in the Supplemental Material section of CIP-003-7 Draft 1 reopens the debate by asserting that LERC exists for a serially-connected low impact BES Cyber System that can be reached from offsite via an IP/Serial Converter that is “...continuing the same communications session from device(s) outside the BES asset boundary to the low impact BES Cyber Systems.” N&ST agrees with the view that the use of protocol converters doing nothing more than mapping IP connections to serial connections does in fact establish “direct” routable communication with “target” serial devices, and we believe the LERC definition should say so (along with a hopefully obvious declaration that IP-capable low impact BES Cyber Systems that can themselves initiate or receive IP connection requests have “direct” connectivity).

Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1	
Answer	No
Document Name	

Comment

As currently proposed, the revisions go beyond clarifying the use of “direct” and create additional compliance burdens and regulatory risk without providing a corresponding increase in the reliability benefits. Below are areas of concern:

1. Removal of the filter: The proposal defines all routable electronic access as LERC. This lessens some uncertainty around whether an entity would have to prove the negative (i.e. there would be far fewer instances where an entity would need to prove that LERC does not exist); however, it does so by making everything LERC and expanding the burden to demonstrate a lack of any routable communication over the BES asset boundary. This requires substantial analysis to identify the presence of LERC at asset locations that entities did not need to analyze under the V.6 Standard.

2. The asset boundary: Exelon appreciates the SDT effort to support applying the requirements for Lows at the BES asset level and using the “asset boundary” as a method to define the BES asset and the point at which communication goes from the outside-in or vice versa. In this concept, Exelon appreciates the flexibility given for Responsible Entities to determine the boundary. The GTB discussion is also useful in support of the concept. However, Exelon finds that the “asset boundary” is not necessary to support the security objective and encourages the SDT to consider methods to simplify the approach. In practice, defining an “asset boundary” creates an additional step to the compliance program, a significantly burdensome one for entities with large numbers of BES assets. In response to Question 3 below, there is a proposal that would eliminate the need and use of the “asset boundary” portion of the approach.

3. Absence of communication to a Low impact BES Cyber System: The proposed definition no longer requires that the routable protocol communication from outside the asset containing low impact BES Cyber Systems have any electronic connection (direct or indirect) to a low impact BES Cyber System(s). The new obligation expands the definition beyond the scope of BES assets under the currently approved Version 6 definition. As a result, under the proposed definition, those assets containing low impact BES Cyber Systems with fully separated (air-gapped) low impact BES Cyber Systems would have LERC even if the only routable connection that crossed the “asset boundary” is to a non-BES Cyber System (e.g. a corporate connection). Moreover, in circumstances where all low impact BES Cyber Assets at a BES asset are separated (air-gapped) and therefore not directly or indirectly accessible from outside the asset containing the low impact BES Cyber System, there is no reliability benefit for creating a list of routable connections at the “asset boundary” and it would become a significant administrative effort to document LERC at such assets. This also seems contrary to the fundamental efforts of the CIP standards to focus protections on BES Cyber Systems. To resolve this issue, if the LERC term goes forward (see proposal in response to Question 3 that could eliminate the need for the glossary term), the existence of LERC should require some electronic routable communication connectivity to a low impact BES Cyber System from outside the asset containing the low impact BES Cyber System. To address this concern, the definition could include an exclusion as follows: “excluding routable protocol communication that does not provide a direct or indirect connection to a low impact BES Cyber System from outside the asset boundary.”

Proposal Q1A: Given the concerns above, Exelon proposes the following approach to return to the currently approved LERC definition. The SDT could address the FERC directive by removing the word “direct” from the definition and update the Section 3 Electronic Access Controls requirement as proposed in the response to Question 3.

Additional Note, “C” in LERC and LEAP retirement: Exelon has no objection to changing the “C” in LERC to “Communication” and would support the revision as part of the proposal. “Communication” is a more accurate representation. Retirement of LEAP would also still be appropriate under the SDT proposal and under the proposals outlined in these comments.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	

Comment

Protecting the Bulk Electric System (BES): Sometimes lost in the drafting process is the objective of the NERC Reliability Standards—to guide and provide the framework to reliably operate the BES. That framework includes operations, planning, design, emergency response, and, as in this case, critical infrastructure protection. There are Standards that succeed in ensuring reliable BES operation and there are Standards that consume entities' resources and offer little incremental improvement to reliability. It is through the lens of reliability and cost to implement we offer comments regarding the Proposed LERC definition.

Concern—Boundary of an Asset: The use of "boundary of an asset" is ambiguous, unclear, and has likely unintended consequences.

The term potentially expands applicability to any routable protocol communication that crosses an asset boundary regardless of a connection to a BES Cyber System or not. See CIP -003- 7 Supplemental Material: LERC Reference Model No

The term is silent as to whether it will be applied equally and consistently across an Entity's BES system.

The term, when considered with the glossary terms incorporated by reference, promotes confusion. Specifically, the undefined term, "asset," and glossary term, "BES Cyber Asset," which is incorporated in the definition of BES Cyber System referenced in the proposed LERC term.

Along those lines, the definition of "BES Cyber Asset" incorporates the glossary term, "Facilities." As an example, in an attempt to provide greater certainty around the undefined term, "asset," Entities and the ERO conceivably could look to the glossary term, "Facilities," to interpret the term. We believe such a scenario would bring too many "assets" into scope and go far beyond the intended use of the undefined term, "asset." We recognize such a scenario is unlikely but it, again, highlights the challenge of ambiguity in the proposed definition.

Concern—Boundary of an Asset, Part Two: The phrase, "crossing the boundary of the asset," is ambiguous and unclear whether it is referring only to an electronic boundary and/or a physical boundary.

If boundary includes physical borders, the challenge of interpreting is easily illustrated by the basic plan of a substation.

A substation has multiple points that constitute a physical boundary. For example, the substation property line, its fence, its gate, a control house or houses, and so forth. Then there are the one-offs—does a low impact BES Cyber Asset mounted on a pole or structure in or outside the substation fence line constitute or establish a boundary? The proposed definition does not offer any guidance in that regard.

Concern—Cost to Implement: We expect that the proposed revision will, initially, not greatly impact the industry because of the widespread use of non-routable serial communication between Real-time Units (RTU) and Energy Management Systems (EMS). However, that would change in the future for companies that begin to incorporate routable protocols for communications between RTUs and the EMS, introducing a significant cost and commitment of resources to secure those communications.

When evaluated against the previous LERC definition, the impact becomes apparent. The previous LERC definition was only concerned with "interactive remote access" or people accessing devices inside the low impact substation and remotely modifying their configuration or exercising control over the Facilities. The previous LERC definition excluded machine-to-machine communications using a routable protocol, like communications between RTUs and the EMS.

The proposed definition's scope broadens to include the machine-to-machine communications by including all routable communication except for non-Control Center BES assets.

Unintended Consequence—Delay and Hamper Transformational Change in Substation Communication Infrastructure: The significant cost to implement the compliance obligations created by the proposed LERC definition revisions will incent companies' continued reliance on outdated serial communication standards to defer the implementation costs.

Beyond the cost deferral, companies continuing to rely on analog telecom connections to substations for serial communication will face the hard truth that the principal telecommunication carriers are losing their experienced workforce that are able to maintain the analog systems. As such, the carriers are placing a premium to maintain analog connections. We are aware of a utility that incurred unexpected expense that pushed their costs 44% over budget—representing hundreds of thousands of dollars—just to support their analog system.

The final analysis becomes a business decision—cost to implement against the premium to maintain analog systems, with both being substantial. If the equation favors keeping the analog systems in place, the incentive is diminished to upgrade.

Concern—Security for Security's Sake: The proposed LERC term may very well apply to every BES Facility, establishing a scope so large, Entities would have to devote significant resources to implement and maintain the LERC established assets without a clear or marginal improvement to the reliable operation of the BES.

It is clear in cyber security—it is impossible to plug every hole and often raises the question, should we even try. The statement should not be read as, "why bother;" it highlights Entities' resources are not infinite and there may be more beneficial uses of those resources to favorably impact BES reliability.

Furthermore, there is the concern trolling in low impact weeds without consideration of the risk may actually decrease BES security by misdirecting Entities' attention and causing them not to see fissures and cracks opening in a larger view of the BES Cyber Systems while required to focus on the weeds.

Even recognizing FERC's directive, there is a reason they call them "low impact" assets. We would highlight the need to evaluate the risk; the resources to implement and maintain; and marginal improvement to BES reliability and security. The implications of scope created by the proposed LERC term are significant, material, and likely have unintended consequences.

Concern—Creates Onerous Compliance Tasks: As a corollary to Security for Security's Sake, discussed above, consider the scenario that would, for all intents and purposes, bring every substation into the scope of applicability. The task to install and maintain firewalls and their associated rules under CIP-005-5 would overwhelm most, if not all Entities.

The scenario and its likely impact highlights, there is a reason they call them "low impact" assets. We question whether requiring firewalls at every substation—as reflected in CIP-003-6, Attachment 2, Sections 2 and 3, evidence language—materially improves BES reliability and security.

Concern—Compliance: The proposed LERC term may convert assets to BES Cyber Assets, bringing CIP-002-5.1 into play and an appreciable increase to compliance obligations.

The proposed LERC term may have the unintended consequence of requiring Entities to create comprehensive BES Facility inventories to evidence compliance under CIP-002-5.1. Whether the proposed LERC term or CIP-002-5.1, evidence would be required to support why an asset is or is not a BES Cyber Asset—a "prove the negative" situation. An inventory is the likely path required by auditors to demonstrate compliance.

Proposal

To address our concern regarding the substantial scope of applicability of the proposed LERC definition, we offer the following:

Suggested Modification, delete "containing":

"A routable protocol communication that crosses the boundary of an asset connected to one or more low impact BES Cyber Systems…"

Suggestion

Conceptually, we do not oppose the use of “boundary of asset;” the term needs to either be defined or, at the very least, set out parameters to better establish a manageable scope. We believe our proposed language is a step toward limiting that potential scope of the proposed LERC term.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	No
Document Name	

Comment

We do not agree with these proposed changes.

(1) ACES appreciates the efforts of the SDT with addressing the FERC directive and providing clarity to the LERC definition. However, simply removing ”direct” and replacing “connectivity” with “Communication” generates additional concerns.

(2) Registered Entities have already incurred infrastructure and labor costs to implement various solutions to address the present LERC definition. This include the insertion of unidirectional devices that would intentionally break the communications streams of bi -direc protocol connections. How will these solutions align with the proposed definition?

(3) The SDT proposes to add “Communication” to the LERC definition without providing additional clarification. Does this unintentionally increase the scope of Cyber Assets and BES Cyber Systems? Which of the following Communication protocols are then in scope?

- Computer access control protocols
- Data interchange standards
- Internet protocols
- Network protocols
- Wireless Application Protocol
- XML-based standards

(4) We question how will an entity implement the new LERC definition if they also have External Routable Connectivity? If these two definitions do not align, we believe additional implementation costs and gaps would be created.

(5) The SDT has identified that LERC is an attribute of a “BES asset.” What definition supports this statement? How will Regional Entities consistently apply this definition?

(6) We believe the proposed definition should be modified to clarify the use of an IP Converter as a serial device. We have observed that each Regional Entity has inconsistently applied this use.

Likes 0	
Dislikes 0	

Response

Tim Kucey - PSEG - PSEG Fossil LLC - 5

Answer	No
Document Name	

Comment

PSEG supports comments of EEI and NPCC TFIST

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

NRECA is concerned that the revisions to the LERC definition go significantly beyond addressing the FERC directive to clarify “direct” in the definition. By making everything LERC and requiring the demonstration of a negative (that a connection was never made), this is an added compliance burden without a demonstrated BES reliability benefit. NRECA believes it’s reasonable to require identification and protection demonstration for communication paths that cross the asset boundary and are for BES purposes. However, those communications that have nothing to do with BES communications (i.e., non-BES assets) should be excluded from scope of LERC. Demonstration of an “air-gap” is essentially a requirement to demonstrate a negative (that a connection was never made) and is overly burdensome and does not have a BES reliability benefit. The revisions could make compliance with security for a low impact facility more difficult than at a medium impact facility.

Given NRECA’s concerns, we strongly encourage the SDT to remove the word “direct” from the currently approved LERC definition – this will address FERC’s directive without unnecessarily expanding the scope of LERC beyond the BES. NRECA does not object to changing the “C” in LERC to Communication.

Likes 0	

Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	

Comment
Cowlitz PUD supports the comments as submitted by APPA and Utility Services.

Likes 0	
Dislikes 0	

Response

Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	No
Document Name	

Comment
The revised LERC definition unintentionally draws into scope routable communications between non-BES Cyber Systems and isolated business only communication networks. As written, LERC would apply to all Cyber Assets at a Low impact location if there was a routable business network present. GCPD recommends the following revisions to the proposed LERC definition for clarity. *Routable protocol communication to or from a low impact BES Cyber System that:* • *crosses the boundary of a BES asset containing one or more low impact BES Cyber System(s),* • *does not include communications between intelligent electronic devices used for time* *tions between non-* *Control Center BES assets containing low impact BES Cyber Systems including,* • *is not limited to, IEC 61850 GOOSE or vendor proprietary protocols.* GCPD is also recommending that with a revised definition of LERC as suggested, that CIP-003-7 Supplemental Material be adjusted to reflect and support this revision.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker

Answer	No
Document Name	
Comment	
Generally, we support the LERC definition revisions made, including the replacement of "Connectivity" with "Communication" within the LERC title. However, we do not support a definition that include connections that have nothing to do with the BES. The tasks of (1) identifying and (2) demonstrating protections regarding all communications paths that cross the asset boundary is overly burdensome. We recommend limiting the scope only to those paths that are used for BES communications or to connect to BES Cyber Assets. Thus, it is our position that communications that have nothing to do with BES communications should be excluded from scope. Furthermore, we find no reason to limit the LERC definition to " vendor proprietary protocols." The function of the communication is not to identify a single example of a standard and assume any other examples are proprietary. Thus, we recommend this provision also be excluded.	
Likes 0	
Dislikes 0	
Response	
Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
Answer	No
Document Name	
Comment	
Hydro One Networks Inc. supports the NPCC RSC's comments on this question in its entirety.	
Likes 0	
Dislikes 0	
Response	
Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Data such as routable protocol communications is routinely transported through low impact substations. Bringing data such as routable protocol communication into scope as a result of the broad definition creates an unnecessary compliance burden. The new definition creates too many complexities and is too broad. As it is written the new definition creates more questions than the clarity it was intended to provide.	
Likes 0	
Dislikes 0	

Response

Michiko Sell - Public Utility District No. 2 of Grant County, Washington - 1	
Answer	No
Document Name	
Comment	

The revised LERC definition unintentionally draws into scope routable communications between non-BES Cyber Systems and isolated business only communication networks. As written, LERC would apply to all Cyber Assets at a Low impact location if there was a routable business network present. GCPD recommends the following revisions to the proposed LERC definition for clarity.

Routable protocol communication ***to or from a low impact BES Cyber System*** *that:*

- *crosses the boundary of* ***a BES*** *asset containing one or more low impact BES Cyber System(s),*
- *does not include communications between intelligent electronic devices used for time* *-se*
  Control Center BES assets containing low impact BES Cyber Systems including,
- *is not limited to, IEC 61850 GOOSE or vendor proprietary protocols.*

GCPD is also recommending that with a revised definition of LERC as suggested, that CIP-003-7 Supplemental Material be adjusted to reflect and support this revision.

Likes 0	
Dislikes 0	

Response

John Bee - Exelon - 3	
Answer	No
Document Name	
Comment	

See Exelon TO Response

Likes 0	
Dislikes 0	

Response

Ruth Miller - Exelon - 5	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Exelon - 6	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
NRG supports the comments submitted by NPCC (Ruida Shu on 9/6/16): We recommend replacing “communication” with “connectivity” because communication may weaken the security of the cyber asset. Securing connectivity protects against all attacks using that network pathway. Only securing against communications path would allow reduced security. Because you can be connected without communicating per the OSI layers. Connectivity and communications are diferent OSI layer, which opens up the possibility of connectivity without communications. This leaves a path for attackers to connect through the asset’s boundary. Otherwise, we agree with the new definition. The definition contains two terms that we suggest should be defined terms as they are fundamental to the meaning of LERC and subsequently critical to meeting compliance requirements of any standards/requirements that use the term. "BES asset boundary" is used in numerous instances within the standard attachments and it is assumed that it is synonymous with the term "boundary of an asset", which is used in the definition of LERC. What is meant by the term is described in the Guidelines and Technical Basis, "Requirement R2,	

Attachment 1, Section 3 - Electronic Access Controls". Because there is no correlation between the Guidelines and Technical Basis of the standard and the LERC definition there is no way to understand the term "boundary of an Asset" when reading the LERC definition. The concept of the asset boundary as used in the LERC definition is critical to the meaning of the term LERC and as such it is critical that it be clear and unambiguous. The only way to do that is through the use of a define term or define it within the LERC definition.

"intelligent electronic devices" is used in the definition and in several instances within the Guidelines and Technical Basis of the standard but it is not a common term to the extent that it is unambiguous. We suggest that the term should be clearly defined as a defined term. The word "intelligent" within the term is very subjective and can be interpreted in many different ways. For example it could be interpreted to mean "artificial intelligence" or it could be interpreted to mean "can perform an action without specific direction". "artificial intelligence implies a very sophisticated level of computing where "can perform an action without specific direction" could be a simple timer.

As both of these terms are paramount to the understanding of the term LERC we suggest that they be appropriatly included as a defined term or defined within the LERC definition.

Previous definition was more clear and resulted in less burden on Registered Entities. The proposed definition adds administrative burden without adding any reliability benefit to the BES. Additionally designating an entire asset as LERC may rope non-BES Cyber Assets into compliance with potential future Standards aimed at protecting LERC assets.

If proposed definition must stay:

Physical demarcation (asset boundary) for logical controls does not make sense. As written it is too prescriptive; owners should be allowed discretion on boundary. We propose to allow Entities to define their own logical boundary or boundaries within a low impact asset, essentially a low impact ESP (LESP). An LESP would allow an entity the ability to narrow the scope of applied controls and regulation to low impact Cyber Systems, as CIP is intended, without involving systems that have no reliability impact. Additionally an entity that only has many Low Impact Systems would still have the ability to label the whole site as an LESP or Low Impact Security Zone (LISZ). The LESP would not carry over typical requirements of ESPs so use of the term LISZ may avoid confusion.

Alternatively, we suggest adding a clause to the definition such that the cross boundary communication must be associated with the functionality or operability of the low impact Cyber Systems to constitute LERC. This eliminates the issues below that arise with the current proposed definition:

- Wireless communications, which have no impact on low impact BCS (data enabled cell phone), create the existence of temporary LERC. Given the prevalence of mobile phones, it is hard to imagine a substation which does not have LERC at some time.
- Air gapped configurations do not have the same risk profile as networked substations, but both will be labeled as LERC, thereby undermining the signaling impact of a LERC label. It also creates administrative burden with no reliability impact.
- Certain assets which contain low and medium impact BCS may be listed as non-ERC and LERC. This is unnecessarily confusing.

Remove phrase “or vendor proprietary protocol”. This incentives entities to adopt vendor proprietary protocols to avoid compliance obligation. Incentivizing diverse protocols will reduce the ability of entities to use compatible devices for security solutions in the future.

Likes 0	
Dislikes 0	

Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	2016 02 BPA_No LERC examples_20160906.pdf
Comment	

From FERC Order 822 paragraph 73: “The Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term “direct” as it is used in the proposed definition.”

While BPA agrees that the proposed definition more clearly aligns with the output of CIP-002-5.1 Requirement R1, Part 1.3, BPA believes this changes the focus from device level language to asset level and vastly increases the number of devices that will be subject to compliance. BPA believes this does not improve security commensurate with the increased burden of compliance.

The change from device level to asset level without regard for connections to BES Cyber Systems will vastly increase the number of assets subject to compliance. At BPA, we estimate that the number of Low Impact assets requiring electronic access controls will increase dramatically. Most of these would require extraneous documentation and tracking for communication that was never intended to be addressed by CIP requirements (e.g., corporate network going to into substations without any access to BES equipment).

Proposal: In order to resolve FERC’s concerns about the ambiguity surrounding the word “direct”, BPA proposes that the new definition be modified to better reflect CIP goals. Some of the following language may prove useful in discussions:

“Routable protocol communication, crossing the boundary of an asset containing one or more low impact BES Cyber System(s), capable* of modification of a BES Cyber System”

*Add to Technical Guidance: “Capable” should not include zero-day attacks, software bugs, etc.

“Routable protocol communication that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), unless all BES Cyber Systems are physically air-gapped from the routable protocol…”

Additional models to show LERC/no LERC examples may be helpful (see attached pdf.)

The exclusion segment is difficult to understand:

- In their FAQ at http://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPV5_FAQs_Consolidated_Oct2015_Oct_13_2015.pdf the authors identify IEC 61850 as “an ethernet based standard” that “can be mapped to a number of protocols.” They acknowledge that some of these protocols are routable and some are not. The proposed LERC language exempting IEC 61850 GOOSE is confusing: If they’re referring to the GOOSE protocol, which is defined in IEC 61850-8-1, it is a layer 2 protocol and is not routable. On the other hand, if they are referring to R-GOOSE, which is defined in IEC TR 61850-90-5, it is a layer 3 protocol and is routable. BUT, the name of the protocol is “R-GOOSE”, not “GOOSE”. LERC’s exemption would be much clearer if (1) it didn’t mention IEC 61850 at all, or (2) if it named R-GOOSE specifically, or (3) if it exempted the entire suite of IEC 61850 protocols used for time-sensitive protection and control functions.
- Furthermore, the exclusion is confused by conflicting phrases “excluding” and “including” within the same sentence. If the examples are kept, the exclusion could be broken into a separate sentence for clarity.

Proposed language:

- Suggestion 1 (preferred): “, excluding communications between intelligent electronic devices used for time functions between non -sensi -Control Center BES ass

- Suggestion 2: “This definition excludes communications between intelligent electronic devices used for time functions between non limited to, IEC 61850 or proprietary protocols.”

Or

- “…excludes communications between intelligent electronic devices used for time Control Center BES assets containing low impact BES Cyber Systems, regardless of the protocol, such as, but not limited to, IEC 61850 R-GOOSE or proprietary protocols.”

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

Modification to LERC definition inadvertently draws into scope routable communications among non-BES Cyber Systems isolated from BES Cyber Systems or BCS communication networks. For example, as written, LERC would apply to a business network-connected desktop computer at a Low impact location--that by itself is not and has no connection to any BES Cyber System--solely because the routable communications from the desktop cross the boundary of the Low impact site. As such, a Low impact asset with BES Cyber Systems that lack any routable connectivity would still have LERC (and thus require the protections of CIP-003-7) if there was a routable business network present. This expansion of scope to include business networks does not appear to be intentional, and greatly expands the scope of LERC under the proposed definition. As a corrective, Seattle City Light suggests additional language for the definition of LERC such as “Routable protocol communication AMONG ONE OR MORE BES CYBER SYSTEM(S) that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), excluding…” (CAPITALS indicate additions).

Also, please clarify if LERC is intended to apply to an entire asset (site) or if on a system-by-system basis. The previous definition of LERC clearly applied to individual BES Cyber Systems, in that one BCS at an asset might have LERC and another at the same asset might not have LERC. The new definition, as written, appears to define LERC as a characteristic of the asset (site) as opposed to a characteristic of a cyber system or a BES Cyber System. Seattle City Light recommends clearly stating whichever approach in intended, and strongly prefers language to retain the existing system-based approach. As such, Seattle recommends adding the following sentence at the end to the LERC definition: “THE PRESENCE OR LACK OF LERC IS EVALUATED INDIVIDUALLY FOR EACH BES CYBER SYSTEM EXISTING AT AN ASSET.”

Finally the “Determining Asset Boundary” discussion in the CIP-003-7 Supplemental Material should be revised to clearly state that 1) routable communications on business networks having no connection to BES Cyber Systems are excluded from LERC, and that 2) LERC is a property of individual BES Cyber Systems and not a property of an asset (site) as a whole.

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No

Document Name	
Comment	
Changing the definition to include “Communication” instead of “Connectivity” and following the basis behind this proposal, all substations containing Low Impact BES Cyber Assets would have LERC (e.g. video surveillance, laptops with wireless cards, and other solutions crossing the asset boundary) and would require electronic access controls. This will be a substantial shift for some entities who were building implementation plans to address LEAP’s at only those sites that had low impact BES Cyber Assets connected via routable connectivity. The new definition would require all sites to have electronic access controls. At minimum, “routable protocol communication” should be changed to “routable protocol connectivity to a BES Cyber System that crosses a BES asset boundary.”	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports comments submitted by Edison Electric Institute. Also, while PacifiCorp understands the justification provided for the approach the SDT took, PacifiCorp believes that the approach adds an increased compliance burden without added benefit to the security of BES, or any assurance that entities will not be asked for a list of BES Cyber Assets at Low Impact BES Assets.	
Likes 0	
Dislikes 0	
Response	
Yvonne McMackin - Public Utility District No. 2 of Grant County, Washington - 4	
Answer	No
Document Name	
Comment	
See commentary submitted by Michiko Sell, Public Utility District No. 2 of Grant County, WA.	
Likes 0	
Dislikes 0	
Response	

ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	Yes
Document Name	
Comment	
Good change that supports alignment with R1 part 1.3 and attachment 1, section 3, Low Impact Rating; bi-directional was removed; unidirectional communication promoted the removal; now a data diode is looked at as a control; focus on controls not on if you have a LERC;	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 1, 5, 3; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
This change is good as "Connectivity" is describing what is commonly understood as a physical layer relationship between devices where as "Communication" does not necessarily assume a direct physical layer relationship, as it can be purely logical. This clarification will help entities better develop points of “communications demarcation” as recommended in other impact categories. Understanding those demarcations will give entities the ability to better monitor changes in subject environments that may result in compliance impacts.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

Burns & McDonnel believes the proposed modifications meet the intent of FERC's instructions from Order 822 and provide Registered Entities (Entity) sufficient flexibility in determining what is LERC. Our only concern is the proposed definition and associated example diagrams continue to allow BES Cyber Systems (BCS) to be on the same logical network segment as non-BCS Cyber Assets, which allows for the potential use of those non-BCS Cyber Assets to become an attack vector (i.e. pivot point) to the BCS Cyber Assets. While outside of FERC's instructions in Order 822, we feel the standard should address the possibility of a pivot attack much like what is has been implemented for High and Medium Impact BCS and the identification of Protected Cyber Assets (PCA) on the same logical network.

Likes 0	
Dislikes 0	

Response

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	Yes
Document Name	

Comment

Occidental Chemical Corporation (OCC) agrees that the concept of direct and indirect access to Low-Impact BES Cyber Systems unnecessarily complicates the assessment of their cyber protections. This differentiation seems to have arisen in CIP v3 in order to develop requirements specific to firewall-protected communications (direct) and remote access communications (indirect). The concept has carried over into CIP v6 – and while it may be appropriate to delve into the details of security controls related to High and Medium-Impact BES assets, it is not the case for Low-Impact facilities.

Likes 0	
Dislikes 0	

Response

Mary Cooper - Alameda Municipal Power - 3,4 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - NA - Not Applicable - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	
Document Name	
Comment	
signing on with NIPSCO comments of Sarah Gasienica	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	
Document Name	
Comment	

WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Julie Ross - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's comments.	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
We support the comments of TransÉnergie.	
Likes 0	
Dislikes 0	
Response	

2. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 2 Physical Security Controls to reflect the retirement of LEAP. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports comments submitted by Edison Electric Institute. Also, while PacifiCorp understands the justification provided for the approach the SDT took, PacifiCorp believes that the approach adds an increased compliance burden without added benefit to the security of BES, or any assurance that entities will not be asked for a list of BES Cyber Assets at Low Impact BES Assets.	
Likes 0	
Dislikes 0	
Response	

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
No, unless the proposed LERC definition removing the LEAP term is revised.	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Without a LEAP, it is now conceivable that there will be all manner of essentially low to no security access points coming into these low discrete BES assets. That along with the noted communications exemption seems to provide for greater attack surfaces. More discretion on the part of entities in terms of security implementations (cost minimization and cultural inertia), will have the net effect of having less security than if LEAP had been retained. From an attacker's standpoint, why would they go after more secure medium substations when there is an abundance of less secure low substations which can net a comparable effect?	

In BPA's view, the retirement of LEAP and expansion of LERC will increase the number of assets included in the ESP. For example, if you have a substation with multiple buildings but (under the existing version of the standard) only one building has LEAP, you must now secure all buildings. This change will have a negative impact on security levels and actually works against Order 822.

BPA proposes that the SDT retain LEAP and address the Commission's instruction to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition.

Likes 0	
Dislikes 0	

Response

Maggy Powell - Exelon - 6

Answer	No
Document Name	

Comment

See Exelon TO Response

Likes 0	
Dislikes 0	

Response

Ruth Miller - Exelon - 5

Answer	No
Document Name	

Comment

See Exelon TO Response

Likes 0	
Dislikes 0	

Response

John Bee - Exelon - 3

Answer	No
Document Name	

Comment

See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
It appears the SDT is moving away from physically protecting a LEAP associated with LERC but now requires physical protection around devices that provide electronic controls and shouldn't section 2 apply only when LERC exists? The intent on whether to protect a "LEAP" that is no longer defined as a LEAP is unclear.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	

NRECA does not object to the retirement of the term LEAP. However, NRECA suggests modifications to Attachment 1, Section 2 that do not require demonstration of compliance with an air-gap and do not require identification of LERC that is not related to BES facilities. NRECA believes that a solution to this concern could be by revising Attachment 1 Section 2 to add the bold/underlined language: “Cyber asset(s), as specified by the Responsible Entity**, if any,** that provide electronic access control(s) implemented for section 3.1.”

Likes 0	
Dislikes 0	

Response

Tim Kucey - PSEG - PSEG Fossil LLC - 5

Answer	No
Document Name	

Comment

PSEG supports EEI comments

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	No
Document Name	

Comment

We do not agree with these proposed revisions.

We believe the proposed revisions only state “The asset” and not “BES assets.” We ask the SDT if there is a difference. If not, we then request the SDT cease using this term in its presentations.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	No
Document Name	
Comment	

: Exelon supports the retirement of the LEAP definition. Exelon identified one concern with the proposed revisions in Attachment 1 Section 2. The language does not make sense for circumstances where air-gapping is used to provide the electronic access control for LERC as permitted by LERC Reference Model 1 -- Physical Isolation. In those circumstances there is no "Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1." Therefore, it is unclear how a Responsible Entity using air-gapping could comply with Section 2 of Attachment 1. To resolve this issue, Section 2 of Attachment 1 should be revised to add the following qualifier: "Cyber Asset(s), as specified by the Responsible Entity, **if any**, that provide electronic access control(s) implemented for Section 3.1." This change would be consistent with the language in Attachment 2 section 2(b) providing the corresponding Measure.

Likes 0	
Dislikes 0	
Response	

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	
Comment	

FMPA supports the comments of American Public Power Association.

Likes 0	
Dislikes 0	
Response	

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	
Comment	

The SDT did not address shared facilities, which is a real concern. Entities should be encouraged to work together to protect BES Cyber Assets, not have to individually protect them “as specified by the Responsible Entity”. In some regions, having multiple owners of asset Facilities, systems, and equipment is very common. This sharing of a single asset becomes even more common in low impact assets. When controlling physical access at the

perimeter of the BES asset, the current language continues to require JRO, CFR, or MOUs. The language should be revised to provide clear guidance in the either attachment 1 or the Guidelines and Technical basis.

The wording of Section 2 suggests that Responsible Entities have to create a list of Cyber Assets, when it is mean to apply only to the Cyber Assets that provide electronic access control for LIBCS.

We recommend moving “as specified by the Responsible Entity” after “that provide electronic access control(s)” to make this intent more clear, i.e., reword as:

“and (2) the Cyber Asset(s) that provide electronic access control(s), as specified by the Responsible Entity, implemented for Section 3.1, if any.”

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company is a member of the Edison Electric Institute (“EEI”) and generally supports EEI’s comments that are being submitted in response to the proposed modifications.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy supports the comments submitted by Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	No
Document Name	
Comment	

The alternate proposal for Section 2 retains an obligation to protect the Cyber Asset(s) interface (reference FERC-approved LEAP definition) and provides flexibility to protect Cyber Asset(s) providing electronic access control(s), for example, if interface is not the concept of the control. This is important to carry over the in-progress V6 implementation into V7.

Alternate proposal: after “(2) the Cyber Asset(s)” insert “or Cyber Asset(s) interface,” As a result of the alternate proposal for question 3, change the reference from “Section 3.1” to “Section 3.” So it reads as: “Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s) or Cyber Asset(s) interface, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3, if any.”

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	

Response

Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	No
Document Name	
Comment	

PSEG agrees with and supports EEI's comments.

Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

The wording of Section 2 suggests that Responsible Entities have to create a list of Cyber Assets, when it is mean to apply only to the Cyber Assets that provide electronic access control for LIBCS.

We recommend moving “as specified by the Responsible Entity” after “that provide electronic access control(s)” to make this intent more clear, i.e., reword as:

“and (2) the Cyber Asset(s) that provide electronic access control(s), as specified by the Responsible Entity, implemented for Section 3.1, if any.”

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

This response depends on the approach ultimately developed by the SDT to address the FERC directive outlined above. Texas RE would note at this time that LEAPs represent a familiar and understood concept, so substituting access point demarcations for other concepts may introduce additional confusion into the Reliability Standards.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CIP-003-7, Attachment 1, Section 2b, as written suggests that the Responsible Entity is required to have a list of Cyber Assets. CenterPoint Energy believes the intent of the requirement is to control physical access to Cyber Assets used to provide electronic access control for low impact BCS.

CenterPoint Energy recommends the following edits:

“(2) the Cyber Asset(s) that provide electronic access control(s) implemented for Section 3.1, as specified by the Responsible Entity, if any.”

Likes 0	
Dislikes 0	

Response

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No
Document Name	
Comment	
SCE agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
See question 1 comment.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	No
Document Name	
Comment	
ITC Holdings disagrees with the retirement of the term LEAP. The term LEAP allows you to delineate which device is performing the electronic access control. By retiring this term it will leave each entity to make up their own term for the device that will perform the electronic access control.	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No

Document Name	
Comment	
While the defined term LEAP simplified Cyber Asset categorization, it is not absolutely necessary. In some regions, such as FRCC, having multiple owners of asset Facilities, systems, and equipment is very common. This sharing of a single asset becomes even more common in low impact assets. When controlling physical access at the perimeter of the BES asset, the current language continues to require JRO, CFR, or MOUs. The language should be revised to provide clear guidance in either attachment 1 or the Guidelines and Technical basis.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Based on our understanding of the new definition of LERC and the retirement of LEAP, OCC expects to use a defense-in-depth approach to provide physical protection for our Low-Impact facilities and our Low-Impact BES Cyber Systems. In our view, the new language in the Physical Security Controls section of Attachment 1 and the guidance section allow for this approach. Although we understand that the drafting team does not govern compliance, OCC would be concerned if our reading of the intent of the modifications is not accurate. If it is, then other Registered Entities and Compliance Enforcement Authorities will be confused as well – leading to inconsistent application of the requirements.	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	Yes
Document Name	
Comment	
Please also see the comments submitted by the National Rural Electric Cooperative Association (NRECA).	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	

Answer	Yes
Document Name	
Comment	
N&ST agrees with the update to CIP-003-6, Attachment 1, Section 2 Physical Security Controls.	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
AZPS is in agreement with the retirement of LEAP.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	

Comment	
Although Austin Energy (AE) agrees with removing the term "LEAP," we believe the SDT should define the term “electronic access control” to remove ambiguity from the proposed Standard. In the Guidelines document, the SDT provides examples of electronic access controls (restricting IP addresses, ports, or services; authenticating users; air-gapping networks; terminating routable protocol sessions on a non-BES Cyber Asset; implementing unidirectional gateways). We recommend the SDT define the term “electronic access controls” (and provide the examples as part of the definition).	
Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	Yes
Document Name	
Comment	
Basically added access control devices to the list to physically protect? No LEAPs now but access controls need physical security;	
Likes 0	
Dislikes 0	
Response	
Yvonne McMackin - Public Utility District No. 2 of Grant County, Washington - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Bradley Collard - SunPower - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michiko Sell - Public Utility District No. 2 of Grant County, Washington - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - NA - Not Applicable - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no NextEra	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Jeffrey Watkins On Behalf of: Eric Schwarzrock, Berkshire Hathaway - NV Energy, 5; - Jeffrey Watkins	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Oliver Burke - Entergy - Entergy Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Emily Rousseau - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 1, 5, 3; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mary Cooper - Alameda Municipal Power - 3,4 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
We support the comments of TransÉnergie.	
Likes 0	
Dislikes 0	
Response	
Julie Ross - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's comments.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	
Document Name	
Comment	
WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	

Answer	
Document Name	
Comment	
signing on with NIPSCO comments of Sarah Gasienica	
Likes 0	
Dislikes 0	
Response	

3. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 3 Electronic Access Controls to require entities to implement electronic access control(s) for LERC, if any, to permit only necessary electronic access to low impact BES Cyber System(s). Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	No
Document Name	

Comment

LERC Reference Model 7 – User Authentication includes a sentence that states “The electronic access control depicted in this reference model may not meet the security objective for controlling device-to-device communication across the LERCdepending on the specific system configuration in place.”. Clarify the sentence by including a specific example that would be compliant versus one that would be non-compliant.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5

Answer	No
Document Name	

Comment

The proposed definition raises more ambiguity than the current definition and goes beyond the direction of the FERC order.

Likes 0	
Dislikes 0	

Response

Emily Rousseau - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)

Answer	No
Document Name	Project 2016-02 sonet.JPG

Comment

It is unclear how to document LERC electronic access controls, especially for physically isolated and logically isolated systems. Do we need to have detailed network drawings? Do we need to label devices and ports for identification during an audit? Can the documentation be a list? Does the list have to identify each LERC individually or just list the electronic access control types implemented at each asset? How is the documentation for larger networks expected to be validated?

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

The proposed revision is not adequately defined or effectively auditable. The expectation defined in the Guidelines and Technical Basis under Determining LERC does not provide adequate definition of the asset boundary. As such, it is unclear what the asset boundary is. Under this guideline, the asset could be defined as the Facilities, systems, and equipment (a set of hardware and Cyber Assets) that is used within the asset, the Cyber Assets that make up the asset, the physical security border of the asset, or the electronic security border of the asset. Depending on the choice made, the results would be very different with respect to what is crossing the boundary and whether serial to IP converters are included. This lack of definition will result in another round of unclear interpretation of the standard. We have seen where this lack of clear definition led us over the past three years in the Lessons Learned program.

If the intent is for the entity to have full flexibility to define the boundary, there is no clear guidance in the standard that this is allowed. There is tremendous flexibility for both entities and auditors. Clear guidance should be provided prior to approving the Standard, especially for low impact generation locations.

Further, would it be appropriate to address additional concerns identified in the FERC NOI by adding a requirement that any LERC that passes information to any high or medium impact ESP utilizing a transmission path that is not exclusively dedicated to communications for use by an Entity or between Entities is not permitted (or at least must be identified so that the risk is recognized)?

Likes 0	
Dislikes 0	

Response

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns

Answer	No
Document Name	

Comment

Comments: We would suggest to the drafting team that some alternative language should be used in reference to the phrase ‘only necessary’ in Section 3. Suggested alternative language as followed:

‘ to permit only necessary as determined by Responsible Entity’ pertaining to Electronic Access Controls’.

Likes 0	

Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

See question 1 comment.

Likes 0	
Dislikes 0	

Response

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

The revised requirement, and accompanying discussion the CIP-003-7 Supplemental Material, is unnecessarily unclear as regards inbound and outbound access for Low impact BES Cyber Systems having LERC, and in this specific regard does not represent an improvement on the existing requriement. To avoid unnecessary confusion, please revise requirement to clarify.

- If both inbound and outbound access are in scope, revise requirement to state so, such as “Implement electronic access control(s) for LERC, if any, to permit only necessary INBOUND AND OUTBOUND electronic access to low impact BES Cyber System(s).”
- If only inbound access is in scope, revise requirement to state “Implement electronic access control(s) for LERC, if any, to permit only necessary INBOUND electronic access to low impact BES Cyber System(s)” (CAPITALS indicate additions).

The “Determining Access Controls” discussion in the CIP-003-7 Supplemental Material similarly should be revised to clearly state whether the term ‘access’ applies to inbound and outbound access or only to inbound access.

Please also indicate if a single electronic access control is sufficient for all sources of LERC existing at an asset (site) or if individual sources of LERC must be individually identified and appropriate controls implemented for each (this point and related matters are further discussed below in comments for Question 4, Measure M2).

Likes 0	
Dislikes 0	

Response

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No
Document Name	
Comment	
SCE agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	No
Document Name	
Comment	
LG&E/KU supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
The proposed revisions to the Low Impact External Routable Connectivity (LERC) definition, retirement of the Low Impact Electronic Access Point (LEAP) and associated changes to the requirements for CIP-003 Attachment 1 Section 2 and 3 represent a significant shift from the currently FERC-approved definitions and requirements. The proposed changes include identifying LERC to non-BES Cyber Assets increasing the scope. Entities are well into their implementation of the approved definitions and requirements. This fundamental shift creates regulatory uncertainty for entities and timing concerns to meet the proposed implementation schedule due to re-work and the volume of assets containing low impact BES Cyber Systems. At best, FERC approval is not likely till near the end of 2017, which will be too late for most entities’ budgeting schedules for work to be completed in 2018 if the revised requirements require budget changes. It’s not logical to vote yes on the non-binding poll until the requirement language is closer.	
Likes 0	
Dislikes 0	
Response	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
The way it is worded does not provide any security benefit. For instance, reference model number 5 is an example that is not represented by the verbiage. We propose, “Implement electronic access control(s) to permit only necessary electronic communications to Low Impact BES Cyber System(s) at assets in which LERC exists.”	
Likes 0	
Dislikes 0	
Response	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes that the registered entities are in the best position to determine the necessary electronic access controls for their specific environment because they own and/or operate the systems. CenterPoint Energy recommends the following edits to CIP-003 Attachment 1, Section 3.1: **“Implement electronic access control(s) for LERC, if any, to permit only necessary electronic access to low impact BES Cyber Systems, as determined by the Responsible Entity.”**	
Likes 0	
Dislikes 0	
Response	

Julie Hall - Entergy - 6	
Answer	No
Document Name	
Comment	
The Supplemental Material qualifies LERC as “an attribute of a BES Asset… without regard to connectivity to Cyber Assets within the BES Asset” and further states that “LERC can exist for a BES Asset even if there is no routable protocol connectivity to any Low Impact BES Cyber System within the BES Asset.” With the statement that LERC can exist without a connection to a Low Impact BES Cyber System, and Attachment 1 Section 3 Part 3.1 requiring the implementation of “electronic access control(s) for LERC, if any”, the risk of an inadvertent increase in scope referenced in the comments in Question #1 above is again evident with this change as controls would be implemented to secure LERC even though there is no LERC *connection* to a Low Impact BES Cyber System. Therefore, Cyber Assets that would normally be considered out-of-scope could inadvertently be included in this	

case. CIP-003-7 R2 requires the implementation of “cyber security plan(s) for its low impact BES Cyber Systems”, and illustrates the anticipated scope of the requirement as being the protection of Low Impact BES Cyber Systems, not LERC. It is requested that additional clarification be added to Attachment 1 Section 3 Part 3.1 to specify that controls must be implemented to protect Low Impact BES Cyber Systems that *participate* in LERC, not for *any instance* of LERC.

Likes 0	
Dislikes 0	

Response

Oliver Burke - Entergy - Entergy Services, Inc. - 1

Answer	No
Document Name	

Comment

I support comments submitted by Entergy's Julie Hall.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE suggests an asset list and/or diagrams is the best way to identify its low impact BES Cyber Systems and possibly confirm electronic access control applied.

Attachment 1 Section 3 potentially conflicts with the note in Requirement R2 since it *does* ask for a diagram or list of implemented electronic access controls.

Texas RE is concerned the actions Section 3 asks entities does not give the full picture. Even though the diagrams would show electronic access control implemented, it would not show the low impact BES Cyber Systems the electronic access control was implemented on.

Likes 0	
Dislikes 0	

Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

In addition to addressing the concerns we mentioned in our answer to question 1, Section 3 should clarify that Responsible Entities should determine whether the electronic access is necessary as they are in the best position to make those determinations because they own and/or operate these systems.

To address these issues, as well as our question 1 and 6 issues, EEI makes an alternative text recommendation for Section 3 below. We encourage the SDT to clearly state the security objective and allow entities to decide how best to provide evidence in the light of the circumstances at their particular assets.

"Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access, based on need as determined by the Responsible Entity, to the low impact BES Cyber Systems that use (1) a routable protocol leaving or entering the asset containing the low impact BES Cyber Systems, if any, and (2) Dial -up Connectivity, if any. This excludes communications between intelligent electronic devices used for time -sen protection or control functions between non-Control Center BES assets containing low impact BES Cyber Systems including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols.

For routable connectivity, electronic access may be controlled using one or more of the following security controls:

- Physical isolation of the low impact BES Cyber System(s) from the external routable protocol, communication, i.e., an air gap
- A uni-directional gateway
- Logical isolation of the low impact BES Cyber System(s) from the external routable protocol communication, which may include an isolated network segment with logical controls, a host-based firewall, network-based access controls, a Cyber Asset that requires authentication and then establishes a new connection to the low impact BES Cyber System, or other method of logical isolation
- A layer 7 application layer break or other protocol break
- Some other electronic access control that does not allow unauthorized access to the low impact BES Cyber Systems from an external user or device

For Dial-up Connectivity, electronic access may be controlled using one or more of the following security controls:

- Dial-back modems
- Modems that must be remotely enabled or powered up
- Modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use
- Some other electronic access control that does not allow unauthorized dial-up access to the low impact BES Cyber Systems from an external user or device"

EEI also raises a concern our members have with regards to the use of "non-Control Center BES" in the current LERC definition and the above alternative language we proposed. We understand that the SDT was trying to address a technical challenge specific to relay tripping schemes that have millisecond time-sensitivities and was trying exclude normal "poll every few seconds" SCADA traffic as "time-sensitive." We agree that a SCADA system that needs to poll every 2-3 seconds should be protected as firewalls can easily accommodate these requirements. However, there may be scenarios where a Remedial Action Scheme could have components (possibly even the controller itself) in a low impact control center that requires sub-second communication capability, which are not compatible with existing electronic access controls. We recommend that the SDT consider this technical challenge to avoid unintended consequences to reliability and/or compliance.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Jeffrey Watkins - Jeffrey Watkins On Behalf of: Eric Schwarzrock, Berkshire Hathaway - NV Energy, 5; - Jeffrey Watkins

Answer	No
Document Name	

Comment

It is unclear how to document LERC electronic access controls, especially for physically isolated and logically isolated systems. Do we need to have detailed network drawings? Do we need to label devices and ports for identification during an audit? Can the documentation be a list? Does the list have to identify each LERC individually or just list the electronic access control types implemented at each asset? How is the documentation for larger networks expected to be validated?

Likes 0	
Dislikes 0	

Response

Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG

Answer	No
Document Name	

Comment

PSEG agrees with and supports EEI's comments.

Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

Suggested wording for Attachment 1 Section 3.1: “Implement technical and/or procedural controls to permit only necessary electronic communications to low impact BES Cyber Systems and to mitigate the risk of unauthorized electronic access to BES Cyber Systems.” Please consider eliminating the

definition of LERC and eliminating reference to LERC in Attachment 1 Section 3. The definition of LERC is too broad, will cause confusion regarding the concept of asset “boundary” and permits risk due to the exclusion of “time-sensitive” communications.

We support the SDT approach of not prescribing how Responsible Entities meet the security objective. The non-exclusive examples described in the Measure and Guidelines are useful.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

It isn’t clear how to document LERC electronic access controls, especially for physically isolated and logically isolated systems. We would be opposed to having to provide detailed network drawings for all Low Impact assets. If a list would suffice then would it require identification of each LERC individually or simply the electonric access control types. How will this information be validated. Lets not forget that these are by definition LOW IMPACT.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

It isn’t clear how to document LERC electronic access controls, especially for physically isolated and logically isolated systems. We would be opposed to having to provide detailed network drawings for all Low Impact assets. If a list would suffice then would it require identification of each LERC individually or simply the electonric access control types. How will this information be validated. Lets not forget that these are by definition LOW IMPACT.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO

Answer	No
Document Name	
Comment	

This represents a significant change from the previous version creating regulatory uncertainty and possible re-work of already completed work for hundreds to thousands of assets depending on the size of the Entity. Entities have already started to implement based on the currently approved version. This level of change creates timing issues and concerns for meeting the proposed implementation schedule. The alternate proposal adds clarity on a layer 7 application layer break using language from the Guidelines and Technical Basis, which was referenced by FERC in Order 822. The alternate proposal also (1) reflects removal of LERC and LEAP definition, (2) keeps the FERC-approved obligations to protect routable and Dial-up Connectivity, (3) removes “user-initiated interactive”, “device-to-device: and “direct” references, (4) retains the concept of “bidirectional” from the FERC-approved LERC definition by using “leaving or entering”, (5) moves time-sensitive protection and control functions exclusion from LERC definition to Att. 1 Section 3 and expands it to include comparable time-sensitive protection and control functions for generation and for possible sub-second communications between a Remedial Action Scheme and a low impact Control Center. (Perhaps time-sensitive or words to that effect needs to be defined.)

Alternate proposal: Each Responsible Entity shall control electronic access, based on need as determined by the Responsible Entity, to low impact BES Cyber Systems that use: (1) a routable protocol leaving or entering the asset containing the low impact BES Cyber Systems, if any, and (Dial-up Connectivity, if any. This excludes communications: (1) between intelligent electronic devices used for time-sensitive protection or control functions between BES assets containing low impact BES Cyber Systems including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols; (2) when there is a layer 7 application layer break or a Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System (A complete security break does not allow access to the low impact BES Cyber Systems from an external user or device); or (3) when there is no bidirectional routable or Dial-up Connectivity to low impact BES Cyber Systems at the asset.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	
Comment	

Duke Energy supports the comments submitted by Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment
Southern Company is a member of the Edison Electric Institute (“EEI”) and generally supports EEI’s comments that are being submitted in response to the proposed modifications.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment
The revisions are not clear. While we agree that only necessary electronic access should be allowed, the definition of ‘asset boundary’ keeps the requirement from being implemented in a straightforward way. It is also uncertain how this guideline will be applied during an audit. The term asset is undefined and there are no provisions for prescribing what that might include. This makes the definition lack clarity and makes it more difficult for entities to determine and protect LERC if it might exist.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment
We would suggest to the drafting team that some alternative language should be used in reference to the phrase ‘only necessary’ in Section 3. Suggested alternative language as followed: ‘ to permit only necessary as determined by Responsible Entity’ pertaining to Electronic Access Controls’.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA supports the comments of American Public Power Association.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST believes the revised requirement statement for electronic access controls (Attachment 1, Section 3) to "permit only necessary electronic access to low impact BES Cyber System(s)" is vague and therefore could be subject to a wide variety of interpretations. Concerns include:

- The phrase, "access *to*" low impact BES Cyber System(s) could be interpreted to mean that only inbound connections to BES Cyber Systems must be controlled. N&ST assumes this is not the SDT's intent, based on the fact several revised "LERC Reference Models" in the CIP -003- 7 D Supplemental Material section describe the use of "inbound and outbound" access controls. N&ST recommends that the Attachment 1 Section 3 requirement for electronic access control retain the existing "inbound and outbound" language so as to avoid controversy over the Standard's intent.

- The revised "examples of evidence" for electronic access controls (Attachment 2, Section 3) lists "authenticating users" as one approach. If an entity authenticates users who are accessing low impact BES Cyber Systems, has the electronic access control requirement been fully addressed? N&ST believes the answer is or should be "No," as authenticating users may not, by itself, fully control inbound access and does not control outbound access at all. LERC Reference Model 7 ("User Authentication") makes note of this very problem with the comment, "The electronic access control depicted in this reference model may not meet the security objective for controlling device -t system configuration in place." N&ST recommends that the requirement statement in Attachment 1 make it explicit that electronic access controls must be applied to both user-to-device and device-to-device communications where LERC exists and one or both of the communicating devices is a low impact BES Cyber System. N&ST also recommends that the "examples of evidence" section for electronic access controls be revised to make it clear that in cases where there are both user-to-device and device-to-device communications via LERC, a combination of controls may be required.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1	
Answer	No
Document Name	
Comment	

Comment 1: The currently proposed language could be read to require electronic access controls for both BES and non-BES Cyber Assets. While Exelon does not think that is the intent of the language, the intent should be clearer. In addition, the order of the assessment and application of the electronic access controls could be better understood with a subtle change in the sequence of the requirement language. Please consider the following revision: "For asset(s) containing low impact BES Cyber System(s) with LERC, if any, implement electronic access controls to permit only necessary electronic access to the low impact BES Cyber System(s)."

Comment 2: Also, continuing the discussion from the response to Q1, Exelon presents the following proposals for SDT consideration in addressing the concerns raised.

Proposal Q3A – Using the LERC definition proposed in Q1 (Q1A –simply remove 'direct'), the following requirement proposal removes the obligation to inventory and maintain evidence of every routable connection at the asset containing the low impact BES Cyber System as well as having to define and support what the Responsible Entity determines is the "asset boundary" for identifying routable connections. Instead this proposal focuses the obligation on the performance of the security objective associated with electronic access controls for the asset containing low impact BES Cyber Systems.

SECTION 3. Electronic Access Controls: Each Responsible Entity shall:

3.1 For asset(s) containing low impact BES Cyber System(s) with LERC, if any, implement one or more of the following method(s) to achieve the objective of applying electronic access control(s) to permit only necessary electronic access to low impact BES Cyber Systems:

- Physical isolation
- Logical isolation
- Host-based inbound and outbound access permissions
- Network-based inbound and outbound access permissions
- Centralized network-based inbound and outbound access permissions
- Uni-directional gateway
- Jump host located within the asset containing the low impact BES Cyber System
- Session termination within the asset containing the low impact BES Cyber System
- Other method(s) to achieve the objective of applying electronic access control(s) for LERC

3.2 Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

Additionally, to support this proposal, LERC Reference Model 7 – User Authentication should be updated to focus on the use of a "jump host" which would meet the security objective of electronic access controls for LERC instead of how the model is written which does not itself necessarily achieve the security objective as stated in the text of the model.

Proposal Q3.2: Alternatively, the following is another proposal that meets the FERC directive to address "direct," aligns the compliance language to the approach used for Section 2 of Attachment 1 for Physical Security and incorporates the concepts from the LERC definition into the obligation language; thereby removing the need for the separate definition. This proposal retains the examples from the GTB that provide electronic access controls.

SECTION 3. Electronic Access Controls: Each Responsible Entity shall control electronic access, based on need as determined by the Responsible Entity, to low impact BES Cyber Systems that use (1) a routable protocol leaving or entering the asset containing the low impact BES Cyber System(s), if any, and (2) Implement authentication for all Dial ity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Communications between intelligent electronic devices used for time able protocol between non Center BES assets containing low impact BES Cyber Systems is excluded from Section 3; including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb

Answer	No
Document Name	

Comment

Concern—Creates Onerous Compliance Tasks: We would reiterate, as detailed in our Question No. 1 comments under the subheading, Security for Security's Sake. When the scenario is considered that would, for all intents and purposes, bring every substation into the scope of applicability and then require Electronic Access Controls (EAC) for each substation, the task to install and maintain firewalls and their associated rules under CIP-005-5 would tax most, if not all Entities, to comply.

We recognize there are offered alternatives but regardless of the EAC, it is a substantial, arduous, and resource consuming activity with a likely limited benefit to BES Reliability.

Again, the scenario and its likely impact highlights, there is a reason they call them "low impact" assets. We question whether requiring firewalls or other Electronic Access Controls at every substation materially improves BES reliability and security.

Proposal

As previously offered, a modification to the proposed LERC term would temper the potential scope of applicability to only routable protocols connected to low impact BES Cyber Systems.

“A routable protocol communication that crosses the boundary of an asset connected to one or more low impact BES Cyber Systems…”	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
We do not agree with these proposed revisions. FERC has a Notice of Inquiry, Docket No. RM15-14-002 and RM16-18-000, that is asking whether air-gapping networks are sufficient for network security. We believe the minimum level of Electronic Access Controls available is insufficient to address these inquiries.	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	No
Document Name	
Comment	
PSEG supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	

NRECA believes the proposed language could be understood to require electronic access controls for BES and non-BES Cyber Assets. The proposed language should be revised to clarify that the scope does not apply to non-BES Cyber Assets. This can be accomplished by specifically addressing only “low impact BES Cyber Systems” in the language in order to remove the ambiguity regarding non-BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	No
Document Name	

Comment

Cowlitz PUD supports the comments supplied by APPA.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker

Answer	No
Document Name	

Comment

In general, we do not support the air gap as an electronic access control mechanism. Demonstration of an "air gap" is a requirement to validate in the negative. In effect, Responsible Entities must provide proof of a connection that was never initiated. For example, the use of a smartphone introduces routable communications that crosses the asset boundary creating LERC. Using the air gap concept, the Responsible Entity must now account for that connection and be able to demonstrate that an air gap exists between it and the low impact BES Cyber Assets. This is overly burdensome. As a result, we propose that the air-gapping concept be excluded from scope.

Likes 0	
Dislikes 0	

Response

John Bee - Exelon - 3

Answer	No
Document Name	

Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Ruth Miller - Exelon - 5	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Exelon - 6	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

The proposed change in language expands the scope but does not reduce the ambiguity as required by 822. There is not a prescribed, measurable process for how an entity can “permit only necessary electronic access to low impact BES Cyber System(s)” and prove compliance without a complete inventory within the asset boundary. BPA believes this means that every asset within a Low BES can conceivably have its own access control of varying sophistication. This will, like Question 2, encourage the least costly compliance-driven controls be put forth as meeting an interpretation of the regulation. The result will be widely varying practice and commensurate security levels. BPA believes this changes the focus from device level language to asset level and vastly increases the number of devices that will be subject to compliance. Again, the decision to do away with a LEAP has a cascade effect in what will likely result in creating less security as multiple devices will be directly reachable via routable communications and each will have to have its own security.

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

The revised requirement, and accompanying discussion the CIP-003-7 Supplemental Material, is unnecessarily unclear as regards inbound and outbound access for Low impact BES Cyber Systems having LERC, and in this specific regard does not represent an improvement on the existing requriement. To avoid unnecessary confusion, please revise requirement to clarify. If both inbound and outbound access are in scope, revise requirement to state so, such as “Implement electronic access control(s) for LERC, if any, to permit only necessary INBOUND AND OUTBOUND electronic access to low impact BES Cyber System(s).” If only inbound access is in scope, revise requirement to state “Implement electronic access control(s) for LERC, if any, to permit only necessary INBOUND electronic access to low impact BES Cyber System(s)” (CAPITALS indicate additions).

The “Determining Access Controls” discussion in the CIP-003-7 Supplemental Material similarly should be revised to clearly state whether the term ‘access’ applies to inbound and outbound access or only to inbound access.

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No
Document Name	

Comment

Based on the proposed definition of LERC, all substations containing Low Impact BES Cyber Assets will have LERC. In this case, and due to the removal of routable protocol access statements, it is unclear what electronic access is required (e.g. remote electronic access versus a Technician directly connecting to a BES Cyber Asset via a serial interface while standing in front of the BES Cyber Asset).

Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	

Answer	Yes
Document Name	
Comment	
Adds EACMS as a required for Low Impact when external rroutable connectivity or Dial Up exists; what does the flexibility look like mentioned on page 30?	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
We believe the SDT should define “electronic access control” to remove ambiguity from the proposed Standard. In the Guidelines document, the SDT provides examples of electronic access controls (restricting IP addresses, ports, or services; authenticating users; air-gapping networks; terminating routable protocol sessions on a non-BES Cyber Asset; implementing unidirectional gateways). We recommend the SDT define the term “electronic access controls” (and provide the examples as part of the definition).	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 1, 5, 3; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
This is good because the criteria that results in a device being classified as a “Low Impact” asset is narrowly formed from a "Reliability Impact" perspective and not from a security perspective. The reliability concern is independent of its security risk to other environments. As so, the emphasis on “controlling access” is a step in the right direction to meaningfully achieving security.	
Likes 0	
Dislikes 0	
Response	

Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Burns & McDonnell has noticed many comments regarding the “implement electronic access control(s)” language of the proposed requirement is causing some concern with Registered Entities (Entity), with most of those comments related to bring into scope non-BES Cyber Systems (BCS). We feel most of those concerns are valid based on a lack of information within the Guidenace and Technical Basis (GTB) section on what has to be identified and to what extent the identification has to be for non-BCS communications. Burns & McDonnell recommends the Standard Drafting Team (SDT) provide additional clarity in the GTB section on what documentation is required for the non-BCS communcations to help guide Entities in the development of their documentation.	
Likes 0	
Dislikes 0	
Response	

Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
AZPS is in agreement with the revision to require implementation of electronic access controls for LERC to permit only necessary electronic access to low impact BCS; however, respectfully requests that examples of such controls (not all inclusive) be provided in Attachment 1rather than as part of the examples of evidence in Attachment 2. Inclusion of examples such as those listed in Attachment 2 - restricting IP addresses, ports, or services; authenticating users; air-gapping networks; terminating routable protocol sessions; and implementing unidirectional gateways - will ensure that entities employ a secure method to protect LERC, which reduces risk to the BES. Additionally, the Supplemental Material section for Requirement R2, Attachment 1, Section 3 - Electronic Access Controls states that “control(s) must allow only “necessary” access as determined by the Responsible Entity and they need to be able to explain the reasons for the electronic access permitted with their electronic access controls …[which] can be documented within the Responsible Entity’s cyber security plan(s) or other policies or procedures associated with the electronic access controls” (CIP-003-6 Redline, Page 32). AZPS respectfully requests that the Standard Drafting Team Supplemental Materials should not add new or different obligations or expectations to requirements, but, rather, clarify them. AZPS respectfully asserts that the statement requiring reasons for permitted electronic access could be interpreted as adding obligations or expectations that are not included in the actual requirement language. Accordingly, AZPS requests that the SDT remove the reference to documentation of or explanation of reasons for electronic access in cyber security plan(s) from the Supplemental Material section.	
Likes 0	
Dislikes 0	
Response	

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	Yes
Document Name	
Comment	

OCC agrees that the identification of the proper boundary for the Low-Impact facility is a much more straight-forward process than attempting to differentiate between direct and indirect access. In our view, this still assures that every communication path that enters or leaves our facility will be properly assessed. We can then determine the most appropriate physical and cyber protections for each, on a case-by-case basis.

OCC is relying heavily on the language in the requirements, measures, and GTB to assure compliance with the requirement. We did not find any gaps in the materials, but would hope that the drafting team captures any new relevant examples that may arise during the review of CIP-003-7.

Likes 0	
Dislikes 0	
Response	

Mary Cooper - Alameda Municipal Power - 3,4 - WECC

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no NextEra	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - NA - Not Applicable - SPP RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michiko Sell - Public Utility District No. 2 of Grant County, Washington - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Yvonne McMackin - Public Utility District No. 2 of Grant County, Washington - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	
Document Name	
Comment	
signing on with NIPSCO comments of Sarah Gasienica	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	
Document Name	
Comment	
WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Julie Ross - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's comments.	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	

Document Name	
Comment	
We support the comments of TransÉnergie.	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

4. Measure M2: The SDT revised the complementary language of CIP-003-6, Attachment 2, Sections 2 and 3 to make the evidential language of the Measure consistent with the revised requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No
Document Name	

Comment

This is based on the response to Q1. The definition needs to be very clear in its requirements so that the appropriate measures can be applied.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker

Answer	No
Document Name	

Comment

More specifically, our concern is with the wording of Attachment 2 Section 3 Paragraph 1. The comma usage seems to distort the meaning of the paragraph. We recommend the following; "Documentation of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; authenticating users; air gapping, gateway, jump host, directional gateways, etc.) showing that LERC at each asset or group of assets containing low impact BES Cyber Systems is confined only to the access the Responsible Entity deems necessary."

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	No
Document Name	

Comment

See Question 3.

Likes 0	

Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA recommends that the SDT provide specific examples of compliance measures when there is no LERC or dial-up connectivity present.	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	No
Document Name	
Comment	
PSEG supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Concern—Compliance: As detailed in our Question No. 1 comments, the proposed LERC term may convert assets to BES Cyber Assets, bringing CIP-002-5.1 into play and appreciably increase compliance obligations. The proposed language to CIP-003-6, Attachment 2, Sections 2 and 3 reinforces our concern that the proposed LERC term may have the unintended consequence of requiring Entities to create comprehensive BES Facility inventories to evidence compliance under CIP -002- 5.1.	

While such inventories are not explicit in CIP-003-6, Attachment 2, Sections 2 and 3, the plain interpretation suggests evidence is basically requiring an inventory of all low impact BES Cyber Assets and how they were determined.

Proposal

Accept *pro forma* schematics and diagrams representative of categories of LERC BES Cyber Systems. For example, if an Entity's 161kv substations all have a LERC connected to a BES Cyber Asset, that the *pro forma* schematic/diagram is sufficient without a comprehensive list.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

In Section 3, there are no measures/documentation identified for the specific case that LERC or Dial-up does not exist. The applications guideline states "[i]n the case where there is no LERC or Dial [illegible] low impact cyber security plan(s)." Please provide specific examples of compliance measures when there is no LERC or Dial-up Connectivity present.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

Attachment 2 Section 3: Documentation – "termination routable protocol sessions on a non-BES Cyber Asset" is not good. This could lead to a "pivot attack" if the non-BES Cyber Asset it compromised. Also what happens if the connection is routed through the non-BES Cyber Asset and back to a BES-Cyber Asset? This would only make sense if the connection terminated at the non-BES Cyber Asset and that asset could only communicate wth the Low Impact BES Cyber Asset. Additionally, we would recommend adding a common after the close parenthesis (in the first sentence) to help improve the grammar structure of the paragraph. Also, we would suggest to the drafting team to add more clarity on what model 7 and model 8 can be used for and the documentation required to support the process.

Likes 0	

Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company is a member of the Edison Electric Institute (“EEI”) and generally supports EEI’s comments that are being submitted in response to the proposed modifications.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy supports the comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	No
Document Name	
Comment	
The proposed change requires evidence of LERC to non-BES Cyber Assets. Alternate proposal: The alternate proposal (see question 3) would require corresponding changes to Attachment 2 measure for Sections 2 and 3 to make it consistent with the alternate proposal revisions.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry

Dislikes 0	
Response	
Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	No
Document Name	
Comment	
PSEG agrees with and supports EEI's comments.	
Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
In addition to our other concerns, the SDT should make it clear that a device that provides electronic access controls, such as in Reference Models 7 and 8, is not considered a BES Cyber Asset. EEI recommends addressing this by adding the following text to M2: “Note: A Cyber Asset that provides electronic access control(s) under R2 is not a low impact BES Cyber Asset.”	
Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	

To the extent that the models are revised per industry comments including those of the SPP RE, this section will need to be modified. The SPP RE is concerned that the allowance of terminating routable protocol sessions on a non-BES Cyber Asset could, depending on the configuration of the intermediate system, enable a pivot attack. Refer to the SPP RE comments regarding Reference Model 8 in response to question 5.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Please see previous comments. Texas RE encourages entities to have an inventory of their low impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CIP-003-7, Attachment 2, Section 2b, as written suggests that the Responsible Entity is required to have a list of Cyber Assets. CenterPoint Energy believes the intent of the requirement is to control physical access to the Cyber Assets used to provide electronic access control for low impact BCS.

CenterPoint Energy recommends the following edits:

"The Cyber Asset(s) that provide electronic access control(s) implemented for Section 3.1, as specified by the Responsible Entity, if any."

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No

Document Name	
Comment	
For each asset or group of assets that contain LERC, documentation showing that communication to Low Impact BCS is confined to only that which the Responsible Entity deems necessary. Examples of this documentation could include representative diagrams or lists of the implemented electronic access controls (e.g., restricting IP addresses, ports, or services; authenticating users, air-gapping networks; terminating routable protocol sessions on a non-BES Cyber Asset; implementing unidirectional gateways).	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
The proposed revisions to the Low Impact External Routable Connectivity (LERC) definition, retirement of the Low Impact Electronic Access Point (LEAP) and associated changes to the requirements for CIP-003 Attachment 1 Section 2 and 3 represent a significant shift from the currently FERC-approved definitions and requirements. The proposed changes include identifying LERC to non-BES Cyber Assets increasing the scope. Entities are well into their implementation of the approved definitions and requirements. This fundamental shift creates regulatory uncertainty for entities and timing concerns to meet the proposed implementation schedule due to re-work and the volume of assets containing low impact BES Cyber Systems. At best, FERC approval is not likely till near the end of 2017, which will be too late for most entities' budgeting schedules for work to be completed in 2018 if the revised requirements require budget changes. It's not logical to vote yes on the non-binding poll until the requirement language is closer.	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	No
Document Name	
Comment	
LG&E/KU believes this needs to be modified based on the change in definition.	
Likes 0	
Dislikes 0	
Response	

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SCE agrees with and supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Erika Doot - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

In Attachment 2, Section 3, examples of evidence "such as representative diagrams or lists of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; authenticating users; air -gappi implementing unidirectional gateways)" where not previously specified could be interpreted to apply some of the same requirements as for high and medium impact BES Cyber Systems. Reclamation is not clear on whether the intent of this revision is to update the requirement. Reclamation requests that the drafting team provide clarification on whether the addition of this language is intended to update R2.

Likes 0	
Dislikes 0	

Response

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

Seattle finds the proposed concept of LERC and the associated controls to be incompetely considered and subject to numerous confusing and/or unintended consequences. If the proposed approach must be adopted, please at least clarify the following questions:

1. If there are multiple sources of LERC at an asset (site), are individual electronic access controls for a BCS required for each source of LERC, or is one blanket access control sufficient? What about the case of an asset (site) having two different sources of LERC: one source being a badge reader system connected to a company-wide network by Ethernet and the other source being a wireless business network to connect

some desktops and a printer. An air gap might be a sufficient and appropriate protection against the Ethernet-based LERC, but by itself would not be so for the wireless LERC. By extension, would every source of LERC need be identified, documented, and controlled?

2. Do the following cases represent violations for Section 3? For one, consider an asset without LERC, which has BCS that lack any capability for routable communications. If someone entered the site with a cellphone that had an activated internet hotspot (perhaps because he or she used the hotspot at home the night before and forgot it was still active), does the temporary introduction of LERC and the lack of any specified LERC control on the BCS constitute a violation? Would it still be a violation if the cellphone itself never entered the asset (site) but the hotspot range (the routable communications) did reach inside the asset (site)? For two, consider an asset (site) with LERC sourced from an ethernet business network. The local BCS is air gapped from the business network. Now if the same hotspot-enable cellphone is brought into (or nearby) the site, introducing wireless LERC, is there a violation? Would it matter if the BCS was inherently incapable of any routable communications?

3. Can prospective electronic access controls for a BCS be specified in advance of knowing the specific source of the LERC (or if there is any LERC at all)? In particular, consider the case of a BCS composed of one or more BCAs that lack the capability to support routable communications. Would it be considered compliant to simply list “air gap” for this BCS without knowing anything at all about the type and/or presence of LERC at the location (asset)?

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

See question 1 comment.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

The statement:

“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.”

We expect that monitoring controls will not control access in the view of NERC CMEP based on Version 5 audit approach identified in the evidence request and will not be accepted as evidence of compliance. As a result, the expectations are unclear. The language in Attachment 1 needs to be updated to permit the use of monitoring as a form of access control

Section 3

There are no measures/documentation identified for the specific case that LERC or Dial-up does not exist. The applications guideline states "[i]n the case where there is no LERC or Dial-up Connectivity, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s)." Does this mean an attestation or statement that there is no LERC or Dial-up Connectivity in an asset sufficient? If not, please provide specific examples of ompliance measures when there is no LERC or Dial-up Connectivity present.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	No
Document Name	

Comment

The language in of CIP-003-6, Attachment 2, Section 3-1 does not properly restrict the applicability to the Low Impact BES Cyber Systems within an asset.

Suggested language:

Documentation, such as representative diagrams or lists of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; authenticating users; air gapping, gateway, unidirectional gateways, etc.) showing that LERC at each asset or group of assets containing low impact BES Cyber Systems, has been limited to the necessary electronic access deemed necessary by the Responsible Entity to Low Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AECI supports the revised measure, which states, “Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to: 1. Documentation, such as representative diagrams or lists of implemented electronic access controls…” Upon analysis of the text in this measure, it appears that a single representative diagram could be utilized as substantiating evidence for several BES assets that share a common configuration. If this was the intention of the SDT, it could relieve entities of added compliance burden related to documenting LERC under the proposed definition. AECI supports the new definition and this approach to demonstrate compliance.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Exelon - 6	
Answer	Yes
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Ruth Miller - Exelon - 5	
Answer	Yes
Document Name	
Comment	

See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
John Bee - Exelon - 3	
Answer	Yes
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
We agree with the proposed revisions.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Attachment 2, Section 3: Please consider using the term “isolating” or “separating” instead of or alongside the use of “air-gapping.” The strict use of the term “air-gap” implies that there are no cables whatsoever connected to a device that allows any communication to or from the air-gapped device. However, it appears that the use of air-gap in the proposed revisions is only referring to communication that is outside of the asset containing	

the low impact BES Cyber System, while there is no air-gap restriction to the Cyber Asset being connected for communication within the asset containing the low impact BES Cyber System. Exelon foresees that there could be some enforcement confusion over this nuance and recommends that the SDT clarify within the GTB to what extent air-gapping as an electronic access control is acceptable.

The revised measures posted for comment would also accommodate all of the proposed language changes presented in questions 1 and 3.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	Yes
Document Name	

Comment

We support the SDT approach of not prescribing how Responsible Entities meet the security objective. The non-exclusive examples described in the Measure are useful.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 5

Answer	Yes
Document Name	

Comment

AZPS is in agreement with aligning the language of the Measure to be consistent with the language of all Requirements.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

No Comment	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Yvonne McMackin - Public Utility District No. 2 of Grant County, Washington - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michiko Sell - Public Utility District No. 2 of Grant County, Washington - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - NA - Not Applicable - SPP RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no NextEra	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Jeffrey Watkins On Behalf of: Eric Schwarzrock, Berkshire Hathaway - NV Energy, 5; - Jeffrey Watkins	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Oliver Burke - Entergy - Entergy Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 1, 5, 3; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	
Document Name	
Comment	
N&ST agrees with the update to Measure M2 to CIP-003-6, Attachment 1, Sections 2 and 3.	
Likes 0	
Dislikes 0	
Response	

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
We support the comments of TransÉnergie.	
Likes 0	
Dislikes 0	
Response	
Julie Ross - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's comments.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	

Answer	
Document Name	
Comment	
WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	
Document Name	
Comment	
signing on with NIPSCO comments of Sarah Gasienica	
Likes 0	
Dislikes 0	
Response	

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides example diagrams that illustrate various electronic access controls at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

We respectfully point out that within the section "Insufficient Access Controls" of the GTB the term LEAP still appears in Reference Models 1 thru 4 and 7. This appears to be an editing error but should be rectified.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5

Answer	No
Document Name	

Comment

Due to the amibiguity of the proposed definition, the examples are confusing especially as the SDT continues to confuse Cyber Assets with Physical Assets.

Likes 0	
Dislikes 0	

Response

Emily Rousseau - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)

Answer	No
Document Name	

Comment

In addition to the Guidelines and Technical Basis diagrams we suggest providing a diagram to illustrate electronic access controls with an example using a multiplex system (SONET) that shares hardware and includes serial non-routable protocol to low impact BES Cyber Assets and Ethernet routable protocol to non-BES Cyber Assets. This configuration is used by many Low Impact entities. See provided diagram. Per this diagram, only the right hand side (which utilizes routable protocol) would have an associated LERC at the boundary whereas the left hand side (which utilizes serial non

routable serial protocol) would have no LERC. Note, the right and left hand side enter the asset boundary on a “shared” (carrying both routable and not routable protocol communications) Optical Fiber cable and utilize a “shared” multiplexer however since the left had side is not routable Similar to LERC Reference Model 2 in CIP-003-7, the nonroutable “low impact BES Cyber System(s) are on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s)”.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

The comment “The term “BES Asset Boundary” is capitalized in the diagrams but it is not a defined term” raises concern. Please use the proper capitalization for the defined terms to prevent confusion.

Reference Models 1 and 2 use the term LERC as defined, however the use of the term in this manner introduces confusion.

Reference Model 1 may need to clarify the use of the term air-gap with respect to wireless communications. While the vast majority of the audience will understand the concept, it may be necessary to ensure the model is understood correctly by some entities. Using the term LERC to highlight communications to non-BES equipment confuses the intent of the requirement. While the intent is clear, the diagram provided does not necessarily meet attachment 3, section 1. Specifically,

“Implement electronic access control(s) for LERC, if any, to permit only necessary electronic access to low impact BES Cyber System(s).”

One valid understanding of the requirement is that access control(s) for LERC is required. Further, the electronic access control(s) shall permit only necessary electronic access to low impact BCS. The diagram, as presented, does not have any electronic access controls on LERC. Even though clearly not the intent, the language allows this interpretation.

Reference Model 2 may need to clarify that the intent is to use a configuration technique such as private VLANs to ensure the model is not misinterpreted. Again, this may be necessary to ensure the model is understood correctly by some entities.

Reference Model 3 should clarify the intent of the firewall is to control logical ports, such as TCP and UDP ports, for inbound and outbound communications. As written in this model, it could be interpreted that any use of Windows firewall on the Cyber Asset, regardless of how effectively configured, meets the expectations of this model.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns

Answer	No

Document Name	
Comment	
ITC likes the visual depictions and the information provided in the supplemental material, however, as indicated in question #2, ITC prefers that these diagrams reflected a demarcation point to the network boundary and ther term LEAP remains effective.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
See question 1 comment.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	No
Document Name	
Comment	
If the new proposed LERC approach is deemed necessary, please include a reference model diagram for Low impact assets that clearly indicates that a routable business network, business network device (such as a printer or desktop), or any other non-BES system that is not connected to any BES Cyber System is out of scope for LERC. Please also clarify that LERC is intended to be a property of an individual BES Cyber System and not a property of an asset (site) as a whole. Please also expand the discussion of LERC and the required controls to address the issues discussed above in Measures question #4 (controls for multiple sources of LERC, temporary/incidental introduction of LERC, pre-specified anti-LERC controls).	
Likes 0	
Dislikes 0	
Response	

Erika Doot - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
In the GTB section, "Determining Asset Boundary" the concept of a "logical border" is describing a physical border for low impact facilities, and not what would normally be referred to as a "logical border." Reclamation requests that the logical border concept be maintained in this section.	
Likes 0	
Dislikes 0	
Response	

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
The Requirement 2 Attachment 1 – Section 3 as well as the Reference Models provided in the GTB require the Responsible Entitiy to list all external routable communications. We recommand focusing only on the external routable communications that could potentially cross a low impact BES network, therefore excluding all communications that are physically isolated from the low impact BES. Doing so, we recommend to remove Reference Model 1 – Physical Isolation, as it significantly increases the effort dedicated to documenting and maintaining the list of LERCs, and does not add security value on the low impact BES itself. *In addition to exclude all pure administrative communications, removing the Reference Model 1 – Physical Isolation will also allow to exclude temporary LERCs, such as data enabled cell phones or contrator wifi network, which have no reliability impact.* *The methodology implicitly suggested with CIP003-7 (and Reference Model 1) seems like a top-down approach, since all external routable communications to a low asset need to be listed to eventually identify how the low impact BCS of an asset are electronically secured.* *We currently use a bottom-up methodology, where we first identify each one of our low impact BCS, and, for each, we verify the existence of external routable communication (LERC). We then ensure an electronic access control for each existing LERC. Changing our methodology for a top-down approach represents important impacts in terms of effort, budget and capability of meeting the due deadlines.*	
Likes 0	
Dislikes 0	
Response	

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment	
Due to the nature of the issues and concerns raised by the industry, the Guidelines and Technical Basis sections will need to be revised.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
The proposed revisions to the Low Impact External Routable Connectivity (LERC) definition, retirement of the Low Impact Electronic Access Point (LEAP) and associated changes to the requirements for CIP-003 Attachment 1 Section 2 and 3 represent a significant shift from the currently FERC-approved definitions and requirements. The proposed changes include identifying LERC to non-BES Cyber Assets increasing the scope. Entities are well into their implementation of the approved definitions and requirements. This fundamental shift creates regulatory uncertainty for entities and timing concerns to meet the proposed implementation schedule due to re-work and the volume of assets containing low impact BES Cyber Systems. At best, FERC approval is not likely till near the end of 2017, which will be too late for most entities' budgeting schedules for work to be completed in 2018 if the revised requirements require budget changes. It's not logical to vote yes on the non-binding poll until the requirement language is closer.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Good recommendation however, it does not align with the verbiage of the requirement. The Supplemental Material should give examples of strict interpretation of the requirements language.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	

Answer	No
Document Name	
Comment	
CenterPoint Energy recommends the STD to make modifications to the Guidelines and Technical Basis section to align with the proposed LERC definition as commented in Question #1.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
The SDT made a minor adjustment that is different than the rest of the standards. Starting on page 26, the header was changed from “Guidelines and Technical Basis” to “CIP-003-7 Supplemental Material”. The term “Supplemental Material” is new; Texas RE believes this is an unnecessary change and raises more questions, than simply leaving it as “Guidelines and Technical Basis”. **Requirement R2, Attachment 1, Section 2 – Physical Security Controls**, page 30, under the last paragraph it states, **“***Monitoring as a physical security control can be used as a complement or an alternative to access control*.” Texas RE suggests removing the statement “or an alternative”. Monitoring alone is not a proper form of access control. **Determining LERC Section**, page 30, Texas RE suggests diagram(s) showing LERC examples would be beneficial given the fact that all the LERC reference models are showing examples of “*various electronic access controls at a conceptual level*.” Can the assumption be made that if one the concepts is being used already, then there is LERC present? **Determining Asset Boundary**, page 31; Texas RE suggests diagram(s) showing examples of asset boundaries would be beneficial.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No

Document Name	

Comment

Tacoma Power supports the APPA comments on this issue.

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	

Comment

The SPP RE offers the following comments with respect to the pertinent section of the Guidelines and Technical Basis: (1) The second sentence of the first paragraph of the guidance for Requirement R2, Attachment 1, Section 2 should be clarified that the reference to “these Cyber Assets” is referring to the Cyber Assets that implement the electronic access control(s). While it should be intuitively obvious, the sentence in its entirety is somewhat awkward and confusing and could be restated for clarity. (2) The last paragraph of the guidance for Requirement R2, Attachment 1, Section 2 states, in part, that monitoring as a physical control can be used as an alternative to access control. The SPP RE disagrees, noting that monitoring is not an effective means to deter unauthorized access, especially when there is low to no probability of a rapid response to an intrusion. A remotely monitored camera or sensor, coupled with a significantly time-delayed response, does not control access, whereas a simple lock on a door is an effective deterrent. Neither will assure against unauthorized access, but the locked door at least is a barrier than must be defeated whereas a monitoring system in the absence of physical access controls offers no impediment to entry. (3) The third sentence of the first paragraph of the discussion on determining the asset boundary allows the Registered Entity to determine the asset boundary based on the physical location of networked Cyber Assets. In the instance where there are networked Cyber Assets (same Local Area Network) well outside of the fence line of the asset, such as cooling water well heads miles away from a generating plant, the Registered Entity would be allowed to define the asset boundary to encompass the remote sites without regard to being able to protect the remote Cyber Assets or the communication paths. (4) The SPP RE does not believe that Layer 2 Virtual LANs, as suggested to be permissible by LERC Reference Model 2, can provide logical network segmentation sufficient to assure no communication can occur between the Non-BES Cyber Assets and the Low impact BES Cyber Systems depicted in the diagram. Network isolation needs to be accomplished at Layer 3, with appropriate access controls. (5) LERC Reference Model 7 calls for authenticating a new session before establishing a connection to a Low Impact BES Cyber System. It is not clear whether this reference model is envisioning an intermediate system (jump host) without all of the accompanying controls required of an Intermediate System for High and Medium impact BES Cyber Systems, or more like the AAA authentication performed upon session initiation by a firewall or other similarly capable device such as that envisioned by CIP-005-3, Requirement R2.4. Clarification is requested. (6) LERC Reference Model 8 needs to clarify that any traffic between the Non-BES Cyber Asset in the DMZ and the Low Impact BES Cyber System must go through the access control device. A dual-homed (back end network) environment that allows unrestricted, direct access between the DMZ Cyber Asset and the BES Cyber Asset should be strictly prohibited whether or not IP Forwarding is enabled. Such a configuration enables a pivot attack that would essentially bypass the protective controls put into place to protect the Low impact BES Cyber System.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	
Comment	
Due to our other concerns raised in these comments, the Guidelines and Technical Basis will also need to be edited.	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS is opposed to including example diagrams as part of the Guidelines and Technical Basis (GTB) section of the standard due to the fact that standards may not be updated frequently enough to reflect the most recent technology changes/options. AZPS is in agreement that example diagrams are a useful resource and would recommend inclusion of such in general standard development guidelines documentation, which would provide the ability for more efficient operational changes. In regards to the specific Reference Models, AZPS offers the following: Reference Model 2 – AZPS does not believe this diagram meets the Requirement as there is no security device/function depicted. AZPS also respectfully requests that the GTB section not contain additional or conflicting language to the requirements to avoid confusion or misinterpretation. Attachment 1, Section 3.1 states that entities must “[i]mplement electronic access control(s) for LERC, if any, to permit only necessary electronic access **to** low impact BES Cyber System(s)” (CIP-003-6 Redline, Page 22, emphasis added). However, GTB Requirement R2, Attachment 1, Section 3 states that electronic access controls are required when “external routable protocol communication (LERC) or Dial-up Connectivity is present **to or from** the asset containing the low impact BES Cyber System(s)” (CIP-003-6 Redline, Page 30, emphasis added). AZPS recommends aligning the language between these two statements.	
Likes 0	
Dislikes 0	
Response	
Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	No
Document Name	
Comment	

PSEG agrees with and supports EEI's comments.

Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

1. Please eliminate the concept of LERC. All electronic communications should have access controls. Reference Model 1 illustrates that absence of routable connectivity is an example of an electronic access control for communications. It also illustrates that the use of non-routable communications functions as an electronic access control. The sections “Determining LERC” and “Determining Asset Boundary” would no longer be needed if the LERC definition is eliminated. Add a discussion of secure deployment of routable time-sensitive communications such as IEC 61850.

2. In general, the Reference Models do a good job of illustrating that entities have flexibility in where and how they choose to implement electronic access controls. However, Reference Model 5 shows communication through a “cloud” that implies an unprotected or shared network. Even if communication is over a VPN, the BES Cyber Systems located at the BES assets could be exposed to probes for open ports and vulnerabilities. Please consider removing the “cloud” graphic and change the final sentence to “Care should be taken that electronic access to the networks at the BES asset where BES Cyber Assets reside can only be through the device controlling electronic access at the centralized location.”

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

In addition to the Guidelines and Technical Basis diagrams we suggest providing a diagram to illustrate electronic access controls with an example using a multiplex system (SONET) that shares hardware and includes serial non-routable protocol to low impact BES Cyber Assets and Ethernet routable protocol to non-BES Cyber Assets. This configuration is used by many Low Impact entities.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
In addition to the Guidelines and Technical Basis diagrams we suggest providing a diagram to illustrate electronic access controls with an example using a multiplex system (SONET) that shares hardware and includes serial non-routable protocol to low impact BES Cyber Assets and Ethernet routable protocol to non-BES Cyber Assets. This configuration is used by many Low Impact entities.	
Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	No
Document Name	
Comment	
Revise the GTB section of the standard to correspond with the proposed revisions in the alternate proposal (see question 3). Also incorporate text from FERC Order 822 paragraphs 67, 69 and 74 regarding implementation of the “layer 7 application layer break” and how NERC clarified it. Revise the posted Reference Models to reflect the proposed retirement of LERC.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy supports the comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Southern Company generally supports the comments filed contemporaneously by the Edison Electric Institute ("EEI"). Southern Company appreciate the opportunity to support EEI's Comments as well as to provide the additional comments regarding references to wireless on page 27, CIP-003-7 Supplemental Material, Part 1.1.2, Organization Stance on the Use of Wireless Networks, Southern Company would prefer further statements and or guidance concerning wireless connectivity.

As proposed, the CIP-003-7 standard implies that wireless protocols should be identified for all wireless communications which cross the Asset's boundary, including both inbound and outbound. Additional clarification should be provided that wireless communications which are configured for the BES Cyber System or associated BES Cyber Asset should be documented. All other wireless communications not configured for a BES Cyber System or associated BES Cyber Asset contained within the defined boundary should be considered out of scope.

Likes 0	
Dislikes 0	
Response	

Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	

The diagrams show examples of "LERC" where it does not exist, which is confusing the definition of LERC with general "external routable connections" (in other words, connections that only include devices that are non-BES Cyber Systems). The definition of LERC is "Low Impact External Routable Communication". One must have a Low Impact BES Cyber System in order to have LERC. Therefore there cannot be LERC without a Low Impact BCS, and therefore you cannot have, as stated in the technical guidance, LERC without connectivity to low impact BES Cyber Systems. If this correction is not made, the simple act of taking a cellphone into a "BES asset" would immediately create LERC. This is unworkable. We understand the challenge of defining LERC, but the focus must remain on low impact BES Cyber Systems and not drag in additional devices that have no bearing on the security of the BES Cyber System. The fact that a computer with an external network connection is in the same room as a BES Cyber System has zero bearing on the security of the BES Cyber System unless the devices are connected in some fashion. Any time there is an "air gapped" network that is sufficiently documented showing zero external connections outside of an asset boundary, that should be all that is required for compliance.

Reference Model 1 does not properly indicate a risk to the BES, and misuses the term LERC.

Reference Model 2 does not demonstrate "LERC" as the Low Impact BES Cyber Systems do not have external routable connectivity. If the SDT wishes to indicate that VLANs or other such technologies are insufficient as protections between logical networks, this information needs to be provided in a

broader context than just switches. Any type of packetized network device is inherently just as risky as a VLAN tag on a properly configured managed switch. However, the mere presence of external routable connectivity on 'any' VLAN on the switch does not constitute LERC.

Reference Model 5, while perhaps useful in some scenarios, can cause extreme problems in others. If an entity were to designate a BES Asset Boundary in a generation plant using the smallest footprint possible (and thereby increasing security due to controlling smaller areas where the BES Cyber Assets actually reside), it would no longer allow the plant to operate. The reason an entity would NOT choose to use the fence line, as suggested in the Supplemental Material, is because this could include additional non-BES Cyber Assets (such as cameras, phones, corporate workstations, etc.) that have no bearing on the security of the BES Cyber System(s). So by choosing a smaller footprint it would prevent the plant from properly communicating on its LAN without having the entire system re-architected. It would then also introduce a single point of failure which would in turn reduce reliability. There should be no additional compliance burden placed on the entity to show how they are protecting "LERC" if there is no bearing on the BES Cyber System. There should also be consistency applied to the Reference Models in order to reduce confusion.

Reference Model 5 also includes the term "Non BES Cyber System" as part of the reference model. This should at least state "Non BES Cyber Asset" to be consistent with the other diagrams.

Reference Model 8 shows a BES Asset Boundary that should only include Low Impact BES Cyber Systems and any other devices on the same network segment. "DMZ" networks should be outside of the BES Asset Boundary. While we agree that the "jump host" idea can be a way to increase security, it can also be abused if it is not properly configured.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

The Guidelines and Technical Basis section needs to be reviewed for consistency in numerous places. There are terms that are capitalized that are not NERC defined terms (BES Asset Boundary, Non BES Cyber System). A review should also be done to make sure the reference models shown are what is needed for the industry to apply in their environments.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No

Document Name	

Comment

Pg 29 Under Requirement R2, Attachment 1, Section 2 – Physical security controls:

“If these Cyber Assets are located within the BES asset and inherit the same controls

outlined in Section 2, this can be noted by the Responsible Entity in either its policies or cyber

security plan(s) to avoid duplicate documentation of the same controls.” This section is confusing and makes no sense. The logic seems circular in protecting the asset.

Pg 31 Determining Asset Boundary

We would suggest to the drafting team to revise the title of the sections to ‘Determining BES Asset Boundary’ for consistency through out the documentation.

LERC Refereence Model 5 – Centralized Network-based Inbound& Outbound Access Permissions

“Care should be taken that electronic access to or between each BES asset is through the electronic access controls at the centralized location.”

We would suggest stronger language instead of ‘Care should be’, this is not allowed under the definition of LERC and should be stated as so.

LERC Refereence Model 8 – Session Termination and Model 7 User Authentication

This model is an example of a piviot attack metntioned for #4. The flow of traffic must stop at the non-BES Cyber Asset and only communicate with the Low-Impact BES Cyber System, otherwise what happens if that non-BES Cyber Asset is compromised?

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA supports the comments of American Public Power Association.

Likes 0	
Dislikes 0	

Response

Michael Buyce - City Utilities of Springfield, Missouri - NA - Not Applicable - SPP RE	
Answer	No
Document Name	
Comment	

Page 26: The header reads, “Supplemental Material”, but the main heading on the page reads, “Guidelines and Technical Basis.” Was it the intent of the SDT to replace the Guidelines and Technical Basis with Supplemental Materials, or make Guidelines and Technical Basis one part of the Supplemental Material? It is the only first-level heading in the Supplemental Material.

Page 29: Requirement R2, Attachment 1, Section 2 – Physical Security Controls, part 1 of the first sentence reads, “The asset or the locations of low impact BES Cyber Systems…” might be better phrased as, “The asset or the locations [containing] low impact BES Cyber Systems…” This should keep with the consistency throughout the requirements.

The Supplemental Material for the proposed CIP-003-7 requirements introduces the phrase “BES assets,” (**Requirement R2, Attachment 1, Section 3 – Electronic Access Controls** (page 30)). This phrase is used interchangeably within the Supplemental Material, and in some instances within the same sentence. Since the phrase, “Assets containing low impact BES Cyber Systems,” is consistently used throughout the currently approved CIP requirements, would the SDT reconsider the use of “BES assets?”

Page 31: The first sentence reads, “As LERC is a BES asset level attribute, it involves a determination by the Responsible Entity of a BES asset boundary for their assets containing low impact BES Cyber Systems.” Considering the recommendation above, to avoid reduncancy, and provide clarity, would the SDT consider revising the first sentence? Below are two recommendations.

- “As LERC is an attribute of an asset containing low impact BES Cyber Systems, it involves a determination of a boundary, by the Responsible Entity, for each asset containing low impact BES Cyber Systems.” or,

- “LERC is an attribute of an asset containing low impact BES Cyber Systems. The Responsible Entity determines appropriate boundary for each asset containing low impact BES Cyber Systems.”

Page 31: The last sentence in the second paragraph reads, “However, this also means that LERC can exist for a BES asset even if there is no routable protocol connectivity to any low impact BES Cyber System within the BES asset.” Was the intention of the SDT to mean “routable protocol communication” in this instance?

There is somewhat of an inconsistent use of the terms: (1) Necessary access; (2) “Necessary” access; and (3) “Necessary electronic access.” Attachment 1, Section 3, part 3.1 uses the phrase “Necessary electronic access.” On page 32, “Necessary” appears within quotes twice. On page 32 in the Concept Diagrams section, and in some of the reference models, the phrase “necessary access” is used when referring to “necessary electronic access.” Could the SDT consider using the phrase “necessary electronic access” when applicable?

The phrases ‘from the LERC’ and ‘across the LERC’ may cause some confusion.

Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No

Document Name	

Comment

N&ST believes that the diagrams in the revised Guidelines and Technical Basis section of the standard are vague and incomplete. In particular, the application of controls is mentioned, but the placement of the control on an individual Cyber Asset – or interface on a Cyber Asset – is not included in the diagram, clouding the ability of the diagram to communicate the intent of the discussion of the placement of the control. N&ST suggests that for each diagram, the exact placement of each control should be indicated. In addition, N&ST suggests that the legend at the bottom of each drawing should be tailored to the types of communications represented by the diagram to support clarity of the relevance and extent of the controls.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	No
Document Name	

Comment

Exelon appreciates the details within the GTB and suggests some further clarifications:

1. The discussion of Requirement R2, Attachment 1, Section 3 -- Electronic Access Controls should be explicit in stating that the determination of the "necessary" electronic access to low impact BES Cyber Systems should be within the discretion of the Responsible Entity, rather than simply "as determined by the Responsible Entity." A dispute between a Compliance Enforcement Authority and a Responsible Entity over whether certain electronic access is "necessary" should not be grounds for finding noncompliance with the Standard. The guidance should be modified to state "The control(s) **will be considered to must** allow only “necessary” access as determined by the Responsible Entity, **if the Responsible Entity can and they need to be able to** explain **the its** reasons for **its decision to identify the** electronic access permitted with **its their** electronic access controls." Additionally, the documentation of the determination can be at a policy or procedure level and is not intended to be at an individual BES asset or low impact BES Cyber System level.

2. If the concept of the “asset boundary” is retained, the section on Requirement R2, Attachment 1, Section 3 -- should leave the identification of the “asset boundary” to the Responsible Entity. As written, the GTB discussion does not sufficiently emphasize the entity determination of the “asset boundary” and help prevent a finding by the Compliance Enforcement Authority that a different “asset boundary” should have been selected. The discussion should end with the statement that "The foregoing list is not exhaustive, and Responsible Entities have the flexibility to identify the “asset boundary” they consider appropriate for their operations."

1. LERC Reference Model 2 - Logical Isolation appears to show a routable protocol into and out of the portion of the network containing the low impact BES Cyber Systems, but the description states that the illustration shows how routable protocol communications into and out of the network containing the low impact BES Cyber Systems are prevented. The diagram should be clarified to match the description.

1. LERC Reference Model 5 - Centralized Network-based Inbound & Outbound Access Permissions states that "The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s)." Depending on the implementation, this

may be a significant change from the current CIP-003-6 and this language should be incorporated in the main body of the diagram, rather than only a reference model. The GTB should state that "This Standard does not require the electronic access control(s) required by Attachment 1 section 3.1 to reside or be applied inside the asset containing the low impact BES Cyber System. The geographic location of **any** Cyber Asset providing electronic access control required for compliance with Attachment section 3.1 is irrelevant so long as the electronic access controls permit only necessary electronic access to the low impact BES Cyber System." The currently approved Version 6 language is specific to the placement of a LEAP being allowed at a location other than the asset containing the low impact BES Cyber System. However, the other currently approved reference models identify that the remaining electronic access controls are applied within the asset containing the low impact BES Cyber Systems. Exelon recommends the SDT clarify if it is permissable that any electronic access controls be applied at a location other than the asset containing the low impact BES Cyber Systems.

1. Exelon supports inclusion of the diagrams in the GTB. We request an additional Reference Model to build on the Reference Model 1 scenario to show routable communication to a BCS and a non-BCS but with the electronic access control going only to the BCS in the asset.

1. Exelon is concerned with the use of the term “air-gap” in the construct of the proposed revisions. The strict use of the term “air-gap” implies that there are no cables whatsoever connected to a device that allows any communication to or from the air-gapped device. However, it appears that the use of air-gap in the proposed revisions is only referring to communication that is outside of the asset containing the low impact BES Cyber System, while there is no air-gap restriction to the Cyber Asset being connected for communication within the asset containing the low impact BES Cyber System. Exelon foresees that there could be some enforcement confusion over this nuance and recommends that the SDT clarify within the GTB to what extent air-gapping as an electronic access control is acceptable.

Proposal: If the Proposed language in Questions 1 and 3 is adopted, the GTB will need to be updated accordingly (i.e. remove assert boundary discussion).

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb

Answer	No
Document Name	

Comment

Concern—CIP LERC Reference Model 1, as offered, basically illustrates any routable protocol crossing the BES Asset Boundary is converted into a BES Cyber Asset. If that is the intent, that reinforces our concerns regarding the potential expansive scope of applicability inherent in the proposed LERC term.

We believe LERC should only reflect connections to low impact BES Cyber Systems and, as such, we question how the diagram has a LERC since a LERC connection is not made to a BES Cyber Asset or System.

Proposal

As previously offered, a modification to the proposed LERC term would temper the potential scope of applicability to only routable protocols connected to low impact BES Cyber Systems.

“A routable protocol communication that crosses the boundary of an asset connected to one or more low impact BES Cyber Systems…”

Incorporating this proposal would require modifying the Model No. 1 illustration or removing it from the GTB.

Likes 0	
Dislikes 0	

Response

Tim Kucey - PSEG - PSEG Fossil LLC - 5

Answer	No
Document Name	

Comment

PSEG supports EEI comments

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

NRECA appreciates the efforts to improve the GTB for R2, and has the following requests for additions to the GTB. First, it would be beneficial if the GTB were revised to show scenarios of dial-up connectivity at low impact facilities. Next, the GTB capitalizes “BES Asset Boundary” in the diagrams, and since this is not a NERC-defined term, it should be corrected to “BES asset boundary.” Lastly, based on all of the comments submitted by NRECA and others, the GTB will need to be updated to address changes made by the SDT.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	No

Document Name	
Comment	
Cowlitz PUD supports APPA comments.	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	No
Document Name	
Comment	
GCPD appreciates the SDTs efforts to clarify the intent of the CIP-003-7 Standard to low impact BES Cyber Systems. However, we are constantly reminded that we will be audited to the Standard Requirement and NOT the Guidelines and Technical Basis. As such, any clarifications to definitions and applicability should be included in the body of the Standard Requirements. Not in an unenforceable section of “supplemental material”.	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	No
Document Name	
Comment	
Please see the answer to question 3 above.	
Likes 0	
Dislikes 0	
Response	
Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	

Comment
The wording related to what devices will require the physical protection is unclear. As it reads it seems the SDT is saying protect a “LEAP” that no longer exists but it is unclear what will be expected to protect these potentially varied electronic access controls.

Likes 0	
Dislikes 0	

Response

Michiko Sell - Public Utility District No. 2 of Grant County, Washington - 1	
Answer	No
Document Name	

Comment
• GCPD appreciates the SDTs efforts to clarify the intent of the CIP-003-7 Standard to low impact BES Cyber Systems. However, we are constantly reminded that we will be audited to the Standard Requirement and NOT the Guidelines and Technical Basis. As such, any clarifications to definitions and applicability should be included in the body of the Standard Requirements. Not in an unenforceable section of “supplemental material”.

Likes 0	
Dislikes 0	

Response

John Bee - Exelon - 3	
Answer	No
Document Name	

Comment
See Exelon TO Response

Likes 0	
Dislikes 0	

Response

Ruth Miller - Exelon - 5	
Answer	No
Document Name	

Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Exelon - 6	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA's position is that the intent of Order 822 is not met by the proposed v7. FERC directed NERC to clarify the definition of LERC. From the GTB on Determining LERC: "With LERC being a BES asset level attribute, it is used as a higher level filter to exclude from further consideration those assets containing low impact BES Cyber Systems that have no routable protocol communications to them from outside the BES asset. Responsible Entities can then concentrate their electronic access control efforts on those BES assets that do have LERC. However, this also means that LERC can exist for a BES asset even if there is no routable protocol connectivity to any low impact BES Cyber System within the BES asset." The diagrams are great illustrations on the diversity, complexity, and ultimately all over the map levels of vulnerability that will represent the state of implementing some form of access control for low BES assets.	
Likes 0	
Dislikes 0	
Response	

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Please include a reference model diagram for Low impact assets that clearly indicates that a routable business network and/or business network device (such as a printer or desktop) not connected to any BES Cyber System is out of scope for LERC. Please also clarify that LERC is intended to be a property of an individual BES Cyber System and not a property of an asset (site) as a whole.	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
LERC Reference Model 1 is based on a general definition of “communications” traversing a LERC boundary as opposed to “connectivity” to a BES Cyber System with an external routable protocol. In addition, “air gap” is not appropriately defined nor a sufficient term in defining segmentation.	
Likes 0	
Dislikes 0	
Response	
Yvonne McMackin - Public Utility District No. 2 of Grant County, Washington - 4	
Answer	No
Document Name	
Comment	
See commentary submitted by Michiko Sell, Public Utility District No. 2 of Grant County, WA.	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC

Answer	Yes
Document Name	

Comment

Is there thought on using encryption for LERC?

For reference Model 7, all previous model focused on acceptable approaches where 7 is more an approach that is NOT acceptable or would require some careful configurations. Consider highlighting the last sentence that indicates this difference in approaches or note that additional controls may be necessary in some way. Consider putting this Model at the end with a different header;

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison

Answer	Yes
Document Name	

Comment

Where applicable, we recommend each Reference Model show the “routable protocol data flow” using the symbols provided.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

As noted in the comment for Question 3, Burns & McDonnell believes additional clarity on to what extent non-BES Cyber Systems (BCS) should be documented, although that does not fully apply to the diagrams.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no NextEra

Answer	Yes
Document Name	

Comment

Where applicable, we recommend each Reference Model show the “routable protocol data flow” using the symbols provided.

Within the section "Insufficient Access Controls" of the GTB the term LEAP still appears in Reference Models 1 thru 4 and 7. This appears to be an editing error.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	Yes
Document Name	

Comment

Hydro One supports comments submitted by NPCC RSC.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	Yes
Document Name	

Comment

We agree with the proposed revisions.

Likes 0	
Dislikes 0	

Response

Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane

Answer	Yes
Document Name	

Comment

Hydro One Networks Inc. supports the NPCC RSC's comments on this question in its entirety.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	Yes
Document Name	

Comment

Where applicable, we recommend each Reference Model show the “routable protocol data flow” using the symbols provided.

Within the section "Insufficient Access Controls" of the GTB the term LEAP still appears in Reference Models 1 thru 4 and 7. This appears to be an editing error.

Likes 0	
Dislikes 0	

Response

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	Yes
Document Name	

Comment

Tri-State appreciates the example diagrams and finds them very helpful. However, we would benefit from a few clarifications/additions: 1) Could you please add one or two that incorporate/reflect Dial-up access? 2) Can you please clarify if “Dial-up” is equivalent to “serial non-routable protocol”, as depicted in Reference Model 1. 3) Can you please clarify whether Dial-up has to have an air gap if non-BES Cyber Assets might be accessible over the same phone system.

Likes 0	
Dislikes 0	

Response

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	Yes
Document Name	

Comment

OCC found the nine examples provided in the GTB section of CIP-003-7 to be helpful and technically accurate. We appreciate the project team’s efforts to provide useful information that will provide guidance and help with our compliance efforts. We expect to reference the examples as support for the strategies employed to protect our Low-Impact BES Cyber Systems.

FERC attributes a great deal of importance to the GTB section. In fact, their directive to modify CIP-003 was based on one example in the GTB (related to Layer 7 application layer breaks) that they believed should be implemented into the requirements. If the Commission finds the GTB to be this compelling, then CEAs should be prepared to find an entity’s program acceptable when implemented in accordance with the GTB.

Cyber protections and modes of attack are evolving rapidly – and protections considered adequate in 2016, may not be in 2018. However, it is impossible for anyone to anticipate a previously unknown hacking strategy, or to immediately upgrade the protective approach once one occurs. Maybe this means that definitive protections must be added to the GTB in an expedited, but controlled manner – the consideration that FERC has recently requested for whitelisting based on the findings from the Ukraine incident may provide a good test case. Everyone understands the urgency, but is it inappropriate to hold entities responsible to expectations that may change based on the most recent cyber event or the interpretation by an audit team.

Likes 0	
Dislikes 0	

Response

John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 1, 5, 3; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Oliver Burke - Entergy - Entergy Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeffrey Watkins - Jeffrey Watkins On Behalf of: Eric Schwarzrock, Berkshire Hathaway - NV Energy, 5; - Jeffrey Watkins	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	
Document Name	
Comment	

signing on with NIPSCO comments of Sarah Gasienica

Likes 0	
Dislikes 0	

Response

Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF

Answer	
Document Name	

Comment

WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI's comments.

Likes 0	
Dislikes 0	

Response

Julie Ross - Austin Energy - 3

Answer	
Document Name	

Comment

I support Andrew Gallo's comments.

Likes 0	
Dislikes 0	

Response

Roger Dufresne - Hydro-Qu?bec Production - 5

Answer	
Document Name	

Comment

We support the comments of TransÉnergie.

Likes 0	
Dislikes 0	
Response	

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) for the revisions made to Sections 2 and 3 of Attachment 2 in CIP-003, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is nine (9) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If not, please provide the basis for your disagreement and an alternate proposal.

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

PacifiCorp supports comments submitted by Edison Electric Institute. Also, the language in the definitions and CIP-003-7 currently out for vote is a substantial rewrite of the requirements as approved by FERC. PacifiCorp cannot afford to wait to begin implementation until a revised standard is approved by FERC, meaning that any approved version that does not allow PacifiCorp to leverage work efforts already completed in alignment with the current FERC approved standard would lead to duplicative effort and costs. Any attempt to compress the overall timeline for implementation could results in a negative impact to the reliability of the bulk electric system.

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No
Document Name	

Comment

Entities have been working towards an implementation plan under the existing definition of LERC and Connectivity, likely resulting in a small number of substations that would actually have LERC. The new definition of LERC addressing Communications brings in all substations containing Low Impact BES Cyber Assets, substantially changing the scope, budget, resources, and schedule to be compliant.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

PacifiCorp supports comments submitted by Edison Electric Institute. Also, the language in the definitions and CIP-003-7 currently out for vote is a substantial rewrite of the requirements as approved by FERC. PacifiCorp cannot afford to wait to begin implementation until a revised standard is approved by FERC, meaning that any approved version that does not allow PacifiCorp to leverage work efforts already completed in alignment with the current FERC approved standard would lead to duplicative effort and costs. Any attempt to compress the overall timeline for implementation could results in a negative impact to the reliability of the bulk electric system.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Because of the increase in scope, BPA suggests a longer implementation period will be required. Due to the need for a complete inventory to be performed, BPA is unable to estimate the amount of time required to implement.

Likes 0	
Dislikes 0	

Response

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No
Document Name	

Comment

Tri-State partially agrees with this proposal. We appreciate the SDT attempting to align the effective dates and establish a single compliance date, but we believe the implementation of CIP-003-6 Attachment 1, Sections 2 and 3, should be deferred/ not enforced. The issue is that the implementation approach for many in the industry would require a significant change under CIP-003-7. This is compounded by large number of BES assets that would be impacted. It seems futile to use significant amounts of resources to prepare for implementation of these sections under the CIP-003-6 standard considering there will be an upcoming shift in direction under the CIP-003-7 requirements. We understand that the SDT cannot request that this portion of CIP-003-6 be deferred; instead we encourage and recommend that NERC staff request a deferral from FERC (or no enforcement) of the implementation of CIP-003-6 Attachment 1, Sections 2 and 3.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
NRG supports the comments submitted by NPCC (Ruida Shu on 9/6/16): Recommend September 1, 2019 because of budget cycles and configuration changes impacting implementation provisions for early adoption of version 7 to align with version 6's enforcement.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Exelon - 6	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Ruth Miller - Exelon - 5	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	

Response	
John Bee - Exelon - 3	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
The change to LERC is significant as well as the approach that will need to be taken in CIP-002 for low impact assets. A longer implementation lead time which would include a minimum of twelve to eighteen months in the event the drafting/approval process takes longer than anticipated is recommended.	
Likes 0	
Dislikes 0	
Response	
Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
Answer	No
Document Name	
Comment	
Hydro One Networks Inc. supports the NPCC RSC's comments on this question in its entirety.	
Likes 0	
Dislikes 0	
Response	

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	No
Document Name	
Comment	
We believe 9 months is not enough time to effectively implement Sections 2 and 3 of Attachment 2 in CIP-003 simply because of the voluminous amont of our assets affected by the updated requirements. That stated, we believe a minimum of 24 calendar months following FERC approval is needed. We are supportive of a single date range for complying with Sections 2 and 3. However, we believe it should be clear that CIP-003v6 Attachment 1 Section 2 and 3 do not need to be implemented until the effective date of v7.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports APPA comment.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA is concerned that nine months is not adequate time for Responsible Entities to assess and implement their compliance program as currently drafted in the revised definition and standard. The Responsible Entities will have significant work to do to survey every BES asset that contains a low impact BES Cyber System and then to comply with the standard requirements. NRECA recommends revising the nine month timeframe to twenty-four months. This extension of time will allow Responsible Entities to focus on the more critical high and medium impact BES assets earlier, while providing extra time for implementation related to low impact BES assets. NRECA is also concerned that Responsible Entities will be working toward compliance with CIP-003-6 while there is potentially significant revisions forthcoming in a Version 7. In order to prevent the inefficient use of Responsible Entity resources, NRECA recommends that the SDT consider revising	

the implementation plan to state that compliance with CIP-003-6 will be deferred and replaced by CIP-003-7 and its associated implementation plan and effective date. If this is outside the scope of work for the SDT, we encourage the SDT to inform NERC leadership of this issue and the actions NERC should take to address this issue. Lastly, for the reasons stated above and in light of the potential for further changes to CIP-003-6 based on comments submitted, NRECA does not support the currently proposed implementation plan.	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	No
Document Name	
Comment	
PSEG supports EEI and NPCC TFIST comments	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
We do not agree with this proposal. We agree that a single effective date for the proposed revisions is necessary. However, Registered Entities have already incurred significant infrastructure and labor costs to implement various solutions that address the present LERC definition. The proposed Implementation Plan also does not acknowledge current efforts made by Registered Entities to address Low Impact BES Cyber System Electronic Access Points (LEAPs). We believe a new effective date should be proposed to account for identifying acceptable solutions, procuring new infrastructure, and installing these modifications on Registered Entity systems. We suggest the latter of September 1, 2019, or the first day of the first calendar quarter that is 18 calendar months after FERC's approval of the standard and NERC Glossary term.	
Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	

Concern. What is being proposed does not consider the challenge of the tasks required or the time needed to implement. Also, it is dependent on the scope created by the eventually accepted and approved LERC definition and CIP-003-7. In light of these variables, additional time is required beyond the proposed Implementation Plan, likely 24 months.

Basis. Entities are already juggling multiple initiatives and implementation of CIP versions 5 and 6 Standards. Additionally, the ONP side of the NERC Standards is seeing material changes and revisions. With many new and revised Standards still freshly borne, the implications and impacts they have or will have on BES security and operations are unknown. Establishing an implementation timeline needs to consider what currently is happening in the CIP and ONP spaces and how they will be impacted by the introduction of additional Standards that likely expand scope, with the potential of converting thousands of assets to BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1	
Answer	No
Document Name	
Comment	

: Exelon appreciates the SDT's attempt to group the deadlines and provide a simple approach to the deadlines. However, Exelon has three concerns:

1. Nine months is not sufficient time for Responsible Entities to assess BES assets and implement a compliance program for the modified definition and revised standard. Substantial new work will be needed beyond updates to procedures or other documentation related to the compliance program. Responsible Entities will have to survey every BES asset they own that contains a low impact BES Cyber System, define the asset boundary, identify the routable protocol connections to the BES asset, document whether any of the routable connections communicate to or from a low impact BES Cyber System across the asset boundary and then identify the appropriate electronic access controls, if needed. The implementation plan should provide for at least 18 months and preferably two years for Responsible Entities to reach full compliance to allow for scheduling site visits, reviews of the communications, determinations of appropriate electronic access controls as well as procurement, testing and implementation project timeframes. Please consider the following suggested wording: "Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7 and the NERC Glossary term Low Impact External Routable Communication (LERC) share become effective on the later of September 1, 2018 or the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable government authority's order approving the standards and NERC Glossary term,

or as otherwise provided for by the applicable government authority." Given the inherent "low impact" nature of these BES assets, a longer implementation period should be acceptable and in the interest of reliability.

2. It is possible that FERC will not approve CIP-003-7 and its implementation plan in time to allow Responsible Entities to transition to CIP-003-7 without first having to implement CIP-003-6. This would be wasted effort and we do not believe that it is the intent or desire of the SDT or the regulators. The SDT could address this as it did for the overlap of V4 and V5. The implementation plan specifically stated that V4 would not become effective, even though the V4 implementation date would have occurred in the interim. "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."

3. Under the proposed Implementation Plan, CIP-003-7, R1.2.3 will become effective April 1, 2017. A plan for LERC will still be in development to accommodate the revised LERC definition and requirements. Entities will be required to develop a plan for LERC according to the CIP-003-6 language. This duplication of effort is not beneficial and it is a drain on the resources responsible for reliability and security.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA supports the comments of American Public Power Association.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Depending on the outcome of the final draft, the Implementation Plan may need to be adjusted to allow more time for the changes.

Likes 0	

Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	
Given the fundamental issues in the current draft, significant confusion by entities is likely to occur. Prior to supporting the implementation, these issues need to be addressed.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company is a member of the Edison Electric Institute (“EEI”) and generally supports EEI’s comments that are being submitted in response to the proposed modifications.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
Hydro One supports comments submitted by NPCC RSC.	
Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy supports the comments submitted by Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO

Answer	No
Document Name	

Comment

The proposed changes create an expansion in scope to include evidence for LERC to non-BES Cyber Assets. Entities must continue implementation with the FERC-approved requirements until such time as the proposed revisions are approved, which at best would be late in 2017. Entities work to implement the currently approved requirements will need to be re-worked based on the new revisions with likely only nine months to complete the re-work for up to thousands of assets containing low impact BES Cyber Assets. By mid-2017, it will be too late to budget for different equipment purchases for work to be done in 2018 if the revisions require any. Therefore, the proposed implementation schedule does not allow enough time to implement the proposed changes. Instead of the latter of Sept. 1, 2018, or 9 months after FERC approval, it should be 24 months after FERC approval.

Alternate proposal: The alternate proposal in question 3 would leverage and extend work on the FERC-approved requirement for lows. Entities could implement lows as approved with certainty work already completed would not have to be redone and would be compliant with revisions that would have later effective dates to address FERC's directive. With this proposal that would minimize re-work, the implementation plan could be the latter of Sept. 1, 2018, or 12 months after FERC approval.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	

Response

Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG

Answer	No
Document Name	

Comment

PSEG agrees with and supports EEI's comments.

Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no NextEra

Answer	No
Document Name	

Comment

Recommend September 1, 2019 because of budget cycles and configuration changes impacting implementation provisions for early adoption of version 7 to align with version 6's enforcement.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

The requirements for LIBCS are in flux, for example, the Standards Drafting team is also adding requirements related to transient cyber assets for LIBCS. Implementing requirements on low impact assets is particularly burdensome due to the sheer numbers of assets, e.g., some of our members have thousands of assets with low impact BCS. Nation-wide there are approximately 55,000 substations, each will require owner/operator visits to make the adjustments. Even minor adjustments to the requirements such the LERC definition changes and adding any new requirements, will require a significant undertaking by the industry. Although we appreciate that NERC and the SDT is trying to rapidly implement these requirements to be responsive to FERC, we caution NERC and FERC to consider potential impacts to the Reliability of the bulk electric system and seek methods to minimize these impacts.

Many of our members have already begun to implement the CIP-003-6 LIBCS requirements and all of our members will have started by January 2017 to be able to make the CIP-003-6 September 2018 effective date. The CIP-003-7 and LERC modifications are due to FERC on April 1, 2017. If FERC takes 3 months to issue a NOPR, 45 days for comments, and 3 months to issue a final rule around November 15, 2017, then companies will have already significantly implemented the CIP-003-6 R2, Attachment 1, Sections 2 and 3. They will then have 10 months to switch from the CIP-003-6 to CIP-003-7 requirements. This produces unnecessary, duplicative implementation requirements for the sake of compliance (adding little to no value to security) and creates regulatory uncertainty for our members in the event regulatory obligations change, creating even more implementation challenges and burdens.

To address these implementation challenges which were caused by FERC approving CIP-003-6 and ordering modifications at the same time, we encourage the SDT to develop a CIP-003-7 approach that enables members who are already implementing CIP-003-6 to continue to do so and remain compliant with CIP-003-7 once FERC approves the new language. We believe our proposed alternative text for question 3 will alleviate this concern.

Another option would be for FERC to stop implementation of CIP-003-6, Sections 2 and 3 until FERC approves the modification, but we do not believe this is under the control of NERC or the SDT.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Oliver Burke - Entergy - Entergy Services, Inc. - 1

Answer	No
Document Name	

Comment

I support comments provided by Entergy's Julie Hall.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6

Answer	No
Document Name	

Comment

Given the proposed implementation plan, governmental authorities will have until November 31st, 2017 to fully approve the proposed revisions without extending the current September 1, 2018 deadline for CIP-003-6 Electronic Access Controls for low impact BCS. The proposed revisions allow entities more flexibility to implement electronic access controls to allow only the required access, which may result in a different solution than the type required under CIP-003-6. The November 31st, 2017 approval date would most likely be past most entities (especially larger entities) design, proposal, and purchasing stages and may result in entities not having the ability to implement the most cost efficient solution. It is requested that the implementation date be rescheduled to be " the later of September 1, 2018 or the first day of the first calendar quarter that is fifteen (15) calendar months after the effective date of the applicable governmental authority's order approving the standard". This would not explicitly extend the deadline immediately for CIP-003-7, but would reduce the timeline of uncertainty for Responsible Entities such that they would have adequate time to consider cost effective solutions.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The requirements for low impact BES Systems are currently in flux and entities will not have certainty regarding low impact requirements until they are approved by the Commission. In addition, the sheer number of assets containing low impact BES Cyber Systems is substantial. It is going to take entities time to implement proper physical and electronic controls at all the various locations. Even minor adjustments to the low impact requirements or LERC definition will require a significant undertaking. CenterPoint Energy believes it is reasonable to request additional time to implement the requirements given that the facilities are low risk to the reliability of the BES. CenterPoint Energy recommends the effective date for CIP-003-7 R2 Attachment 1, Section 2 through 3 to be delayed two years after FERC approval.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
The proposed revisions to the Low Impact External Routable Connectivity (LERC) definition, retirement of the Low Impact Electronic Access Point (LEAP) and associated changes to the requirements for CIP-003 Attachment 1 Section 2 and 3 represent a significant shift from the currently FERC-approved definitions and requirements. The proposed changes include identifying LERC to non-BES Cyber Assets increasing the scope. Entities are well into their implementation of the approved definitions and requirements. This fundamental shift creates regulatory uncertainty for entities and timing concerns to meet the proposed implementation schedule due to re-work and the volume of assets containing low impact BES Cyber Systems. At best, FERC approval is not likely till near the end of 2017, which will be too late for most entities' budgeting schedules for work to be completed in 2018 if the revised requirements require budget changes. It's not logical to vote yes on the non-binding poll until the requirement language is closer. At a bare minimum, the 9 calendar month minimum implementation time should be increased to 24 months in case entities need to revise or significantly expand their programs.	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	No
Document Name	

Comment
LG&E/KU supports EEI's comments. It is very challenging and resource intensive to meet one standard and then have a major component of that standard (e.g., the LERC definition) change. This requires additional expenditure of time and money to meet the new standard. There is the potential that V6 would be effective on 9/1/2018 and industry would then have to meet the V7 changes by 1/1/2019. This timing would be problematic. LG&E/KU recommends that, if approved, the V6 effective date be moved forward to the V7 date, similar to the move of V5 from 4/1/16 to 7/1/16. Additionally, this change combined with changes for TCA at Low are making the attachment to CIP-003 a requirement within itself. LG&E/KU suggests removing this from CIP-003 and creating a new standard (CIP-012) with its own implementation date that addresses all the Low requirements.

Likes 0	
Dislikes 0	

Response

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment
SCE agrees with and supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison

Answer	No
Document Name	

Comment
Recommend September 1, 2019 because of budget cycles and configuration changes impacting implementation provisions for early adoption of version 7 to align with version 6's enforcement.

Likes 1	New York State Reliability Council, 10, ADAMSON ALAN
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
See question 1 comment.	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Given the fundamental issues in the current draft, significant confusion by entities is likely to occur. Prior to supporting the implementation, these issues need to be addressed.	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	No
Document Name	
Comment	
We suggest that Version 7 be implemented instead of the effected requirements in Version 6 in order to prevent confusion and an unnecessary expenditure of resources.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

AZPS is in agreement with the current Implementation Plan timeline as proposed provided that the significant scope increase about which it raised concerns in its earlier comments does not result. AZPS notes that should a significant scope increase as mentioned in the response to Question No. 1, implementation under the proposed implementation plan would be unnecessarily challenging.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	Yes
Document Name	

Comment

Although the implementation period may be reasonable, Texas Re requests the SDT provide a justification of the proposed implementation window. This is particularly important given that the proposed changes serve solely to clarify existing compliance obligations regarding the identification and development of access controls for low impact BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

No comment

Likes 0	
Dislikes 0	

Response

David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC

Answer	Yes
Document Name	

Comment

No Comments	
Likes 0	
Dislikes 0	
Response	
Yvonne McMackin - Public Utility District No. 2 of Grant County, Washington - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michiko Sell - Public Utility District No. 2 of Grant County, Washington - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - NA - Not Applicable - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Jeffrey Watkins On Behalf of: Eric Schwarzrock, Berkshire Hathaway - NV Energy, 5; - Jeffrey Watkins	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Emily Rousseau - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 1, 5, 3; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mary Cooper - Alameda Municipal Power - 3,4 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
We support the comments of TransÉnergie.	

Likes 0	
Dislikes 0	
Response	
Julie Ross - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's comments.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	
Document Name	
Comment	
WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	
Document Name	
Comment	
signing on with NIPSCO comments of Sarah Gasienica	
Likes 0	
Dislikes 0	

Response

7. If you have additional comments on the proposed revisions to address the FERC directive regarding the LERC definition that you have not provided in response to the questions above, please provide them here.

John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6

Answer	
Document Name	

Comment

FERC Order 822 wanted mor information on the term “direct” not through it out,

Likes 0	
Dislikes 0	

Response

David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC

Answer	
Document Name	

Comment

The comments expressed herein represent a consensus of the views of

members of the SERC Critical Infrastructure Protection Committee only and should not be construed as the

position of SERC Reliability Corporation, its board, or its officers.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	
Document Name	

Comment

AE believes the SDT should define “asset.” Based on the “Low Impact” criteria in CIP-002, we believe the SDT should define the term “Asset” as follows:

-- Control Centers and backup Control Centers

-- Transmission stations and substations

-- Generation resources

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

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

-- For Distribution Providers, Protection Systems specified in Applicability Section 4.2.1 of CIP-002.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

From a formatting perspective it would be helpful to use a consistent approach to paragraph and section numbering. There is a mixture of numbers, bullets, and no numbering at all. A consistent number format is very helpful when trying to reference parts or sections of the document in attachments 1 & 2. We suggest you use the same format as is used in the main standard body.

Likes 0	
Dislikes 0	

Response

Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6

Answer	
Document Name	

Comment

signing on with NIPSCO comments of Sarah Gasienica

Likes 0	
Dislikes 0	

Response

Emily Rousseau - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)

Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	
Document Name	
Comment	
Regarding non-binding VRF/VSL poll, it is inconsistent with the risk based methodology for an entity that updates it's high and medium impact cyber security policy after 15 months but prior to 16 months to have a lower VSL, but the same entity that fails to update the low impact cyber security policy in 15-16 months to have a medium VSL.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	
Document Name	
Comment	
WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI's comments.	
Likes 0	
Dislikes 0	
Response	

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	
Document Name	
Comment	
ITC Holdings requests that NERC place items related to electronic boundary protection in CIP-005, not CIP-003. The same should apply to physical protections of low. Low requirements should be placed in the standard that closely matches the medium requirements. Transient devices should be in their own standard (i.e., CIP-012). The CIP-003 standard should not be a parking lot for newly developed requirements.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
See question 1 comment.	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	
Document Name	
Comment	
Transient LERC(s) should be addressed in this Standard or in response to the FERC directive to address Transient Cyber Assets at Low Impact. The Standard should address dynamic connectivity into low impact substations. This may include Transient Cyber Assets, mobile substations, intermittent session based communication, and cellular network connections.	
Likes 0	
Dislikes 0	
Response	

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
Due to the several comments and issues raised regarding the LIBCS, the SDT may consider separating Low Impact BES Cyber Systems from CIP-003, and instead create a new standard, or revise CIP-002-5.1, to include LIBCS specific requirements.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	
Comment	
Burns & McDonnell has noticed many comments regarding the “asset boundary” part of the proposed definition is causing some concern with Registered Entities (Entity), with most of those comments related to what is the boundary and could there be differences of opinion on what is the boundary at audit time between the Entity and Audit Teams. We feel the information in the Guidance and Technical Basis (GTB) section of proposed CIP-003-7 has sufficient information to indicate what could be the “asset boundary” and using a practical approach in determining the boundary there should be no question as long as the Entity clearly documents how they arrived at the identification of the boundary. We feel it would be beneficial if the GTB text provided some guidance on how the boundary could be documented to reduce concerns that their determination of the boundary would be questioned by Audit Teams.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
These standards are still ambiguous and would therefore be subjective to the auditor.	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
The current effective date of CIP-003 R1.2.3 requiring a Cyber Security Plan for “Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-Up Connectivity” is April 1, 2017. CenterPoint Energy believes that the Cyber Security Plans for Low Impact BCS in R1.2.3 is dependent upon the definition of LERC and the requirements for CIP-003, Attachment 1, Section 2 and 3 that are currently in flux. CenterPoint Energy recommends that the effective date for CIP-003 R1.2 to align with the effective dates for CIP-003-7, Attachment 1, Section 2 and Section 3. With the ongoing modifications to the low impact BES Cyber Systems requirements, the SDT should consider removing the low impact BES Cyber Systems requirements from CIP-003 and creating a new standard.	
Likes 0	
Dislikes 0	
Response	
Julie Ross - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's comments.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE suggests that “routable protocol(s)” and/or “routable communication(s)” should be defined in the NERC Glossary of Terms and examples given within the definition.

Texas RE ultimately believes that low impact BCAs should be within an Electronic Security Perimeter (ESP). Texas RE would like to reference the purpose statement in CIP-005-5, which reads, “*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*.”

Although not directly within the scope of this project, Texas RE encourages the drafting team to review the Violation Time Horizons set forth in the Standard. From an Enforcement perspective, Violation Time Horizons have a significant impact on the ultimate penalty determination. As such, the SDT may wish to consider the current Operations Planning time horizon set forth in the Standard and articulate a basis for this conclusion.

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	
Document Name	

Comment

The SPP RE respectfully offers the following two comments: (1) The SPP RE believes there is a significant gap in the revised requirements and accompanying definition of Low Impact External Routable Communication (LERC). Unlike the requirements for High and Medium Impact BES Cyber Systems, there is no concept of a Protected Cyber Asset due to the absence of an Electronic Security Perimeter. While the requirement for electronic access controls would conceivably protect non-BES Cyber Assets connected to the same routable network, there is no requirement to protect such Cyber Assets from unauthorized physical access. The requirement is to control physical access, based on need as determined by the Responsible Entity, to the asset or the locations of the low impact BES Cyber Systems within the asset. To the extent that non-BES Cyber Assets are collocated with Low Impact BES Cyber Systems, physical protections will be afforded. However, with the provision in the “Determining Asset Boundary” section of the Guidelines and Technical Basis to expand the “asset boundary” beyond the “fence line,” coupled with the option to control physical access only to the locations of the Low Impact BES Cyber Systems as opposed to protecting the asset in total, non-BES Cyber Assets could reside within the defined asset boundary but not within the physical protection zones permitted by the Standard. This gap introduces an unacceptable risk of attack that would allow the malicious actor ready access to the unprotected Cyber Assets and thus to the connected network, bypassing the electronic access controls designed to protect the Low Impact BES Cyber Systems. (2) The SPP RE has repeatedly encountered the argument that data traffic passed over Layer 2 networks is not routable communication. There is a significant difference between routable communications and routing networks. Layer 3 (routable) traffic encapsulated with Layer 2 headers for transmission over a Layer 2 network segment does not result in non-routable communications. It is the presence of network (not MAC) addresses in the Layer 3 header of the data packet that makes the communication routable. This should be clarified in the Guidelines and Technical Basis section of CIP-003-7, or the term should become a defined term in the NERC Glossary.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI greatly appreciates the work of the Standards Drafting Team and the NERC staff. In additon to our comments submitted under the other questions, we offer the following additional comment. Given our concerns regarding the ongoing modification to the LIBCS requirements, the SDT may want to consider removing the low impact requirements from CIP-003 and create a new standard.	
Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no NextEra	
Answer	
Document Name	
Comment	
Transient LERC(s) should be addressed in this Standard or in response to the FERC directive to address Transient Cyber Assets at Low Impact. From a formatting perspective it would be helpful to use a consistent approach to paragraph and section numbering. There is a mixture of numbers, bullets, and no numbering at all. A consistent number format is very helpful when trying to reference parts or sections of the document in attachments 1 & 2. We suggest you use the same format as is used in the main standard body. The Standard should address dynamic connectivity into low impact substations. This may include Transient Cyber Assets, mobile substations, intermittent session based communication, and cellular network connections.	
Likes 0	
Dislikes 0	
Response	
Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	
Document Name	
Comment	

PSEG agrees with and supports EEI's comments.

Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	
Document Name	

Comment

CIP-002 should be split into two separate standards. R1, R1.1, and R1.2 are planning functions and require a great deal of hair splitting because the deliverable is not clearly defined in the standard. R1.3 and the rest of the standard is about cyber security. Planning engineers don't typicall know cyber security and cyber security people don't typically know transmission systems. No one wants to take responsibility for a standard and analysis that they have no other need to know. Rewriting the standard to separate R1, R1.1, & R1.2 from R1.3 and R2 would streamline the compliance effort tremendously.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	
Document Name	

Comment

CIP-002 should be split into two separate standards. R1, R1.1, and R1.2 are planning functions and require a great deal of hair splitting because the deliverable is not clearly defined in the standard. R1.3 and the rest of the standard is about cyber security. Planning engineers don't typicall know cyber security and cyber security people don't typically know transmission systems. No one wants to take responsibility for a standard and analysis that they have no other need to know. Rewriting the standard to separate R1, R1.1, & R1.2 from R1.3 and R2 would streamline the compliance effort tremendously.

Likes 0	
Dislikes 0	

Response

Roger Dufresne - Hydro-Qu?bec Production - 5

Answer	
Document Name	
Comment	
We support the comments of TransÉnergie.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	
Document Name	
Comment	
The proposed solution to address the FERC directive must allow entities to leverage and extend work already completed to meet the currently approved CIP version 6 requirements as work continues to comply with the revised requirements solution for CIP version 7. The implementation plan must allow adequate time to complete the CIP version 7 changes taking into consideration the large volume of lows.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	
Document Name	
Comment	
Hydro One supports comments submitted by NPCC RSC.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	

Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	
Thank you to the SDT for all of your hard work and dedication.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	
Document Name	
Comment	
Kansas City Power and Light Company endorse the comments offered by Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	
Document Name	

Comment
(1) We are concerned the Implementation Plan makes no mention of current efforts to address LEAPs. What guidance is available for documenting and testing LEAPs? How will Regional Entities conduct audits during the period identified within the Implementation Plan? What actions should Registered Entities follow during this period? (2) We believe the SDT should remove the Interchange Coordinator and Interchange Authority functions from the list of applicable functional entities, as these functions were retired in 2015. (3) We thank you for this opportunity to comment.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	
Document Name	

Comment
In regards to the non-binding VRF/VSL poll, NRECA would like to point out an inconsistent use of the VSLs. As currently drafted, updates to a high or medium impact cyber security policy after 15 months, but prior to 16 months is assigned a low VSL, but the same entity that fails to update its low impact cyber security policy in the same timeframe is assigned a medium VSL. This is not consistent with NERC's risk-based focus on standard development and should be revised to assign a low VSL for the failure to update it low impact cyber security policy during the same timeframe. NRECA appreciates the time and effort of the SDT.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3	
Answer	
Document Name	

Comment

Cowlitz PUD commends the work by the SDT, and supports the general direction being taken.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker

Answer	
Document Name	

Comment

Please note, we are in full agreement and support of comments submitted by the NRECA. In addition, we have several concerns regarding communications that pass through an asset boundary. We are concerned that communications will pass through the asset boundary but will not terminate on anything inisde the boundary (i.e. fiber cable passing through). We are also concerned about identifying asset boundaries for shared facilities because we are under the impression that both entities have to account for all coummunications. In the event that one of the entities' is not a NERC registered entity, we are conerned that we would need to account for all communication paths including those that have nothing to do with the BES. We recommend limiting the scope only to those paths that are used for BES communications or connect to BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane

Answer	
Document Name	

Comment

Hydro One Networks Inc. supports the NPCC RSC's comments on this question in its entirety.

Likes 0	
Dislikes 0	

Response

Johnny Anderson - IDACORP - Idaho Power Company - 1

Answer	
Document Name	

Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
John Bee - Exelon - 3	
Answer	
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Ruth Miller - Exelon - 5	
Answer	
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Exelon - 6	
Answer	
Document Name	
Comment	

See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	
Document Name	
Comment	
NRG supports the comments submitted by NPCC (Ruida Shu on 9/6/16): Transient LERC(s) should be addressed in this Standard or in response to the FERC directive to address Transient Cyber Assets at Low Impact. From a formatting perspective it would be helpful to use a consistent approach to paragraph and section numbering. There is a mixture of numbers, bullets, and no numbering at all. A consistent number format is very helpful when trying to reference parts or sections of the document in attachments 1 & 2. We suggest you use the same format as is used in the main standard body. The Standard should address dynamic connectivity into low impact substations. This may include Transient Cyber Assets, mobile substations, intermittent session based communication, and cellular network connections.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
From FERC Order 822 paragraph 73: “The Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term “direct” as it is used in the proposed definition.” BPA believes the proposed changes to LERC expand the amount of items included, and do not directly address the ambiguity of the term “direct”, as directed by the Commission.	

The decision to do away with LEAP, though understandable from an economic standpoint, would have profound implications on access control implementation and enforcement.

Expansion of scope is counterproductive to the protection of the BES cyber assets.

BPA proposes that the SDT retain LEAP and address the Commission's instruction to "provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition."

Likes 0	
Dislikes 0	

Response

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

PacifiCorp supports comments submitted by Edison Electric Institute. Also, while PacifiCorp understands the justification provided for the approach the SDT took, PacifiCorp believes that the approach adds an increased compliance burden without added benefit to the security of BES, or any assurance that entities will not be asked for a list of BES Cyber Assets at Low Impact BES Assets.

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	

Document Name	
Comment	
In general, focus on protection of control communications versus non-critical communications. Also, some of the Reference Models may be incorrect in the labelling of non-routable versus routable protocols (e.g. Reference Model 1 left-hand side).	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	
PacifiCorp supports comments submitted by Edison Electric Institute. Also, while PacifiCorp understands the justification provided for the approach the SDT took, PacifiCorp believes that the approach adds an increased compliance burden without added benefit to the security of BES, or any assurance that entities will not be asked for a list of BES Cyber Assets at Low Impact BES Assets	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	
: PacifiCorp supports comments submitted by Edison Electric Institute. Also, the language in the definitions and CIP-003-7 currently out for vote is a substantial rewrite of the requirements as approved by FERC. PacifiCorp cannot afford to wait to begin implementation until a revised standard is approved by FERC, meaning that any approved version that does not allow PacifiCorp to leverage work efforts already completed in alignment with the current FERC approved standard would lead to duplicative effort and costs. Any attempt to compress the overall timeline for implementation could results in a negative impact to the reliability of the bulk electric system.	
Likes 0	
Dislikes 0	
Response	

Additional comments received from John Babik of JEA

1. Definition: The SDT replaced the term *Low Impact External Routable Connectivity* with *Low Impact External Routable Communication (LERC)* and revised the definition such that it is relevant to the type of communication that occurs crossing the boundary of the BES asset that contains the low impact BES Cyber Systems. This more clearly aligns with the output of CIP-002-5.1 Requirement R1, Part 1.3. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

Yes:

No: NO

Comments: Low Impact External Routable Communication (LERC) – A routable protocol communication that crosses the boundary of an asset containing one or more low impact BES Cyber Systems, excluding communications between intelligent electronic devices used for time-sensitive protection or control functions between non-Control Center BES assets containing low impact BES Cyber Systems including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols.

NERC SDT has stated that in this revision, the term Low Impact External Routable Connectivity has been changed to Low Impact External Routable Communication (LERC) and simplified so that it is an attribute of a BES asset concerning whether there is routable protocol communications across the asset boundary without regard to 'direct vs. indirect' access that may occur.

However the new definition add to further confusion as it has added the term “crosses the boundary of the asset”. This terminology will require that even BES assets where no routable communication to BES cyber asset, direct or indirect exists, entity will be required to provide evidence to demonstrate the negative, that means absence of communication path to the BES cyber asset. Rather than reviewing the the BES Cyber Asset/System connectivity, it will the obligated to review connectivity across the asset as prove that the BES connectivity is restricted. There are significantly high quantity of BES Cyber Assets with Low BES Cyber asset, and this definition will put considerable burden on the entity to prove the its compliance obligation.

It will be highly recommended that the definition should be revised to limit application to BES Cyber Assets where Low BES Cyber Assets utilizes routable communication , direct or indirect, to communicate with other Non-BES cyber assets within the BES asset or outside the BES Asset.

Additional comments received from Ruben Robles of Salt River Project

1. No

SRP sees the “…boundary of an asset…” as an arbitrary concept. The Guidance and Technical Basis does not provide a framework to determine the “asset boundary.” It simply provides examples of what an asset boundary may be. SRP appreciates that the SDT provided the flexibility by allowing the Responsible Entity to define the BES asset boundary. However, more clarification is needed. It is unreasonable to create controls, policies, processes, and procedures around a concept that relies on an arbitrary idea. Additionally, if the asset boundary is meant to be defined by the Responsible Entity, then it should also be a NERC defined term with so much hinging on that concept.

The term “intelligent electronic devices” is ambiguous. There are many definitions of what is thought to be an intelligent electronic device. It would seem best to use the term Cyber Asset if that is what is meant so as to avoid ambiguity.

SRP agrees with Seattle City Light. SRP also has a network for non-operational devices such as printers and desktops at assets “…containing one or more low impact BES Cyber System(s)” that cross the boundary of the asset. The new definition does not explicitly exclude those networks. As the LERC definition reads, if an asset has at least one BES Cyber System, then all routable protocol communication that crosses the boundary of the asset, with said BES Cyber System, is in scope. SRP does not believe this was the intent of the SDT and would ask the SDT to edit the suggested definition revision to reflect the true intent.

LERC brings more devices into scope at the lows than the BCA concept does at the mediums. An example of this at SRP is that there may be a transformer bushing monitor at a medium that is not in the ESP and does not impact the BES in order to result as a BCA. Therefore, the transformer monitor is not burdened by all of the efforts for compliance. However, at a low site, the transformer monitor would be brought into scope as requiring evidence of compliance and the processes to create and maintain that evidence. The same can be stated for dissolved gas monitors, temperature monitors, weather stations, and the many other devices that have no impact on the BES at all. This creates an unnecessary burden and cost simply for compliance.

2. Yes

SRP agrees with removing the term and appreciates the SDT for providing clearer wording.

3. Yes

SRP agrees with the revision and appreciates the SDT for clarifying “inbound and outbound bi-directional routable protocol access” as simply electronic access. SRP further appreciates the SDT for providing example controls in attachment 2. However, SRP also agrees with the comment made by Dominion Resources, Inc., and would appreciate clarification of the referenced verbiage in Model 7.

4. Yes

No comments

5. No

SRP echoes the comments made by Seattle City Light and would appreciate a model diagram clearly indicating a network used purely for non-operational traffic as out of scope for LERC. Additionally, SRP is requesting a model diagram explaining LERC for technologies such as Multiprotocol Label Switching (MPLS) or Carrier Ethernet used for Communication Networks

SRP also agrees with the comment made by Independent Electricity System Operator and identified many uses of “LEAP” shown in graphics. SRP is assuming this to be an oversight and understands the SDT will remove any reference to the term “LEAP.”

SRP also finds it confusing that the SDT uses the term “BES assets” in the Guidance and Technical Basis as well as the Standard Development Timeline. This term is defined on page 1 of the Guidance and Technical Basis as “any assets containing low impact BES Cyber Systems”. SRP suggests that the SDT not create informally defined terms when describing impacted assets.

6. No

9 months does not allow adequate time for the budgeting process or procurement of the infrastructure needed in addition to the planning and coordination of the installation of new architecture required to support the standard. Additionally the peak loads in the summer months do not support the ability to install new infrastructure between May through August.

CIP-003-6 was approved by FERC on Docket No. RM15-14-000 on 1/21/2016. The compliance date for CIP-003 Attachment 1, Sections 2 and 3 was set for September 1, 2018 per the Implementation Plan for CIP 5 Revisions, dated January 23, 2015. This means Responsible entities were provided 32 months in order to execute what was needed for compliance under CIP-003-6. In order to avoid duplicate or unnecessary effort and expense, implementation would not begin until the approval of CIP-003-7. The revised implementation plan is now only providing 9 months after approval of CIP-003-7 to implement.

SRP is requesting the same 32 months for implementation of CIP-003-7 that was afforded prior. This would set the effective date at August 1, 2020 or the first day of the first calendar quarter that is thirty-two (32) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority.

7. SRP agrees with the comment made by Austin Energy stating "asset" should be a NERC defined term. SRP appreciates that the SDT attempted to do so in the Guidance and Technical Basis. However, if the term is being used to specifically reference something that is called out in the standards and requires controls, then it should be formally defined.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2016-02 Modifications to CIP Standards

Consideration of Comments

Initial Comment Period

October 21, 2016

RELIABILITY | ACCOUNTABILITY




Consideration of Comments – Introduction

The following are the ballots associated with this comment report:

- 2016-02 Modifications to CIP Standards CIP-003-7 IN 1 ST
- 2016-02 Modifications to CIP Standards CIP-003-7 Implementation Plan IN 1
- 2016-02 Modifications to CIP Standards CIP-003-7 Non-binding Poll IN 1
- 2016-02 Modifications to CIP Standards New Term/Definition (Low Impact External Routable Communication)

There were 76 sets of responses, including comments from approximately 169 different people from approximately 126 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages. All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. If you feel there has been an error or omission, you can contact the Director of Standards Development, Steve Noess (via email) or at (404) 446-9691.

The standard drafting team (SDT) appreciates industry comments on the revisions to the CIP Reliability Standard. The SDT considered the comments submitted during the initial posting of revisions developed in response to the LERC directive and the SDT adapted its revision approach for the second proposal currently posted. During the development of the revised standard prior to posting, the SDT made it a priority to conduct outreach as modifications were made to the standards. The SDT has conducted several face-to-face meetings and continues its rigorous conference call schedule to further develop draft revisions to the standard, Implementation Plan, Violation Risk Factors (VRFs), and Violation Severity Levels (VSLs).

On January 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 822 Revised Critical Infrastructure Protection Reliability Standards. In this order, FERC approved revisions to version 5 of the CIP standards and also directed that NERC address each of the Order 822 directives by developing modifications to requirements in CIP standards and the definition of Low Impact External Routable Connectivity (LERC), or the SDT shall develop an equally efficient and effective alternative. To address concerns identified in Order 822, FERC directed the following:

- Develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability.
- Develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).

- Develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule, to the LERC definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

Response to Comments – Summary Responses

The SDT has carefully reviewed and considered each stakeholder comment and has revised language where suggested changes are consistent with SDT intent and industry consensus. Also, several commenters suggested non-substantive language changes. The SDT has carefully considered each such comment and has implemented non-substantive revisions to further clarify the language where needed. Moreover, the SDT has made several clarifications to align the language more closely with SDT intent and industry consensus. The SDT has addressed each comment and has provided below, in summary form, and has provided a response to each of the seven questions.

Questions Proposed to Industry

1. Definition: The SDT replaced the term Low Impact External Routable Connectivity with Low Impact External Routable Communication (LERC) and revised the definition such that it is relevant to the type of communication that occurs crossing the boundary of the BES asset that contains the low impact BES Cyber Systems. This more clearly aligns with the output of CIP-002-5.1 Requirement R1, Part 1.3. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

2. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 2 Physical Security Controls to reflect the retirement of LEAP. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

3. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 3 Electronic Access Controls to require entities to implement electronic access control(s) for LERC, if any, to permit only necessary electronic access to low impact BES Cyber System(s). Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

4. Measure M2: The SDT revised the complementary language of CIP-003-6, Attachment 2, Sections 2 and 3 to make the evidential language of the Measure consistent with the revised requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides example diagrams that illustrate various electronic access controls at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) for the revisions made to Sections 2 and 3 of Attachment 2 in CIP-003, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is nine (9) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If not, please provide the basis for your disagreement and an alternate proposal.

7. If you have additional comments on the proposed revisions to address the FERC directive regarding the LERC definition that you have not provided in response to the questions above, please provide them here.

Consideration of Comments – Summary Responses

Question 1: Definition – Low Impact External Routable Communication (LERC)

Summary Response

1 .Definition: The SDT replaced the term Low Impact External Routable Connectivity with Low Impact External Routable Communication (LERC) and revised the definition such that it is relevant to the type of communication that occurs crossing the boundary of the BES asset that contains the low impact BES Cyber Systems. This more clearly aligns with the output of CIP-002-5.1 Requirement R1, Part 1.3. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal

Expanded Scope

Several stakeholders noted that the revised LERC definition unintentionally draws into scope routable communications between non-BES Cyber Systems and isolated business only communication networks. As written, LERC would apply to all Cyber Assets at a Low impact location if there was a routable business network present.

The SDT updated the proposal for LERC to reflect that the Responsible Entity is to permit only necessary inbound and outbound electronic access for any communications: between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber Systems (revised Attachment 1, Section 3.1); using a routable protocol when entering or leaving the asset; and expanded the Guidelines and Technical Basis with examples of electronic access controls for low impact BES Cyber System(s). Those communications that do not meet the criteria of being "between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber Systems" or "using a routable protocol when entering or leaving the asset" are now clearly out of scope in the revised draft language.

Concerns with the Approach to Addressing FERC Directive

Several commenters expressed concern that current solutions being implemented won't be able to be utilized. As currently proposed, the revisions go beyond clarifying the use of "direct" and create additional compliance burdens and regulatory risk without providing a corresponding increase in the reliability benefits.

The concept now being proposed by the SDT attempts to move the concepts from the currently approved definition of LERC into Attachment 1 while adding the clarity directed by FERC. The SDT believes that this modification will allow entities the freedom to continue to utilize methodologies already being implemented for the previously approved definition of LERC while providing a clear security objective for those electronic access controls.

Boundary of an Asset

Some commenters noted that the term “boundary of an asset” used in the definition needs to be better defined as opposed to leaving the interpretation up to the reader. The guidance in the Standard itself offers reasonable suggestions that all appear to extend no further than the physical property boundary of the asset.

In the new proposed draft language, the SDT moved the concepts in the currently approved LERC definition into Attachment 1, and also removed the reference to the boundary of an asset. The proposed language now ensures all requirement language for electronic access controls takes place at the asset level to be consistent with previously approved CIP-003-6 language. In addition, the SDT added provisions into the Guidelines and Technical Basis to assist entities in determining if in-scope routable communications exist. These guidelines outline that Responsible Entities have flexibility in how to make the determination of which Cyber Asset(s) communicating with low impact BES Cyber System(s) are outside the asset containing low impact BES Cyber System(s) including providing suggestions for defining an electronic boundary or a physical boundary to help determine when protections need to be applied. This approach gives Responsible Entities flexibility in implementation due to differences that may arise based on environment or asset type.

Communications

Several commenters noted that by changing the definition to include “Communication” instead of “Connectivity” and following the basis behind this proposal, all substations containing Low Impact BES Cyber Assets would have LERC (e.g. video surveillance, laptops with wireless cards, and other solutions crossing the asset boundary) and would require electronic access controls. This will be a substantial shift for some entities who were building implementation plans to address Low Impact Electronic Access Points (LEAP) at only those sites that had low impact BES Cyber Assets connected via routable connectivity.

The SDT updated the proposal for LERC to reflect that the Responsible Entity is to permit only necessary inbound and outbound electronic access for any communications: between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber Systems (revised Attachment 1, Section 3.1);using a routable protocol when entering or leaving the asset; and expanded the Guidelines and Technical Basis with examples of electronic access controls low impact BES Cyber system(s). The SDT decided to leave "communications" within the proposed Attachment 1 language to clarify both wired and wireless paths that meet the above need to be protected as such, and concluded that "connectivity" potentially could be interpreted to refer to only physical connections. The SDT believes that the proposed modifications allow entities the flexibility to define protection methodologies appropriate for their environment, including any work already completed for the previous concept of LERC, including the implementation of LEAPs.

Intelligent Electronic Devices

Several stakeholders commented that the term “intelligent electronic devices” is ambiguous. There are many definitions of what is thought to be an intelligent electronic device. It would seem best to use the term Cyber Asset if that is what is meant so as to avoid ambiguity.

The phrase "intelligent electronic devices" is currently a part of the approved LERC definition located in the Glossary of Terms. This portion of the currently approved definition was not part of the scope of the SDT revisions, and as such, remains in the newly proposed draft language for Attachment 1.

Question 2: Retirement of Low Impact Electronic Access Point (LEAP)

Summary Response

2. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 2 Physical Security Controls to reflect the retirement of LEAP. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Retirement of the defined term "LEAP"

After posting draft 1 of CIP -003-7, commenters expressed concern that retiring the term LEAP from the NERC Glossary of Terms and removing it from the standard would cause confusion by removing a familiar and understood concept. Additionally, some commenters expressed concern that retiring the term LEAP would have the net effect of having less security than if LEAP had been retained.

After a review of the comments provided, the SDT proposed that the terms Low Impact External Routable Connectivity (LERC) and LEAP be retired and removed from R2 and all applicable sections of Attachment 1 & 2. In the next revision of the standard, the SDT has simplified the requirements for electronic access controls for asset(s) containing low impact BES Cyber Systems so that it is an attribute of the asset. The SDT modified the requirements to permit only inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls, unless that communication meets the exclusion language. The defined term LEAP is no longer necessary because the SDT changed the requirement from requiring a LEAP to requiring electronic access controls.

Additionally, since the SDT is removing the term LERC, the exclusion language that was previously in the definition of LERC was integrated into the Attachment 1, Section 3.1 requirement. Furthermore, the asset boundary concept and the physical isolation reference model have been removed from the Guidelines and Technical Basis. The SDT believes that the revisions to the requirement language have increased the clarity of the requirement while still achieving the applicable security objectives.

Physical Protections for Cyber Assets Providing Electronic Access Controls

Commenters expressed concern that retiring the term LEAP from the NERC Glossary of Terms and removing it from the standard would cause uncertainty related to physical protections of Cyber Assets that provide electronic access controls implemented for Section 3.1, if any. Commenters stated that Responsible Entities could clearly identify LEAPs and provide physical protections as required by Section 2 of Attachment 1.

After a review of the comments provided, the SDT proposed that the terms Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) be

retired and removed from R2 and all applicable sections of Attachment 1 & 2. The SDT has simplified the requirements for electronic access controls for asset(s) containing low impact BES Cyber Systems so that it is an attribute of a BES asset. The SDT modified the requirements to permit only inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls, unless that communication meets the exclusion language. The defined term LEAP is no longer necessary because the SDT changed the requirement from requiring a LEAP to requiring electronic access controls.

Pursuant to Section 2, physical security controls are required for (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s) that provide electronic access control(s) implemented for Section 3.1, if any. The SDT believes that the revisions to the requirement language have increased the clarity of the requirement while still achieving the applicable security objectives. Additionally, further guidance related to Section 2 has been provided in the revised Guidelines and Technical Basis.

Shared Facilities

Several commenters expressed concern that controlling physical access at the perimeter of the asset causes issues for Responsible Entities that have shared or jointly owned facilities. Commenters stated that the current language continues to require JRO, CFR, or MOUs and that the language should be revised to provide clear guidance in the either attachment 1 or the Guidelines and Technical basis.

After consideration of the comments provided, the SDT revised the language in Section 3, the corresponding measure, removed the asset boundary concept, and removed the physical isolation reference model. The SDT believes that these revisions provide added clarity that will reduce the compliance burden for Responsible Entities that are owners of shared facilities. Unfortunately, there are numerous implementations at shared or jointly owned facilities that cannot be addressed in the Attachment or Guidelines and Technical Basis. The SDT believes that the revision to the requirement language provides added clarity that will reduce the compliance burden for entities that are owners of shared facilities.

Physical Protections for Electronic Access Controls (if any)

After posting draft 1 of CIP-003-7, commenters expressed concerns that the wording of Section 2 suggests that Responsible Entities have to create a list of Cyber Assets, when it is meant to apply only to the Cyber Assets that provide electronic access control for low impact BES cyber systems. Commenters provided alternative wording placement for the language of Section 2 to provide enhanced clarity.

The SDT agrees with the comments provided, that Responsible Entities must document and implement methods to control physical access to (1) the asset or the locations of low impact BES

Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Section 3.1, if any. If the Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls outlined in Section 2, this can be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

After a review of comments provided, the SDT revised the language in Section 3, the corresponding measure, removed the asset boundary concept, and removed the physical isolation reference model. The SDT believes that these revisions provide added clarity that will reduce the compliance burden for Responsible Entities and will simplify the requirements for electronic access controls.

Question 3: Electronic Access Controls

Summary Response

3. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 3 Electronic Access Controls to require entities to implement electronic access control(s) for LERC, if any, to permit only necessary electronic access to low impact BES Cyber System(s). Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

Insert Summary Response

Asset Boundary

Several stakeholders commented that there is a lack of clarity regarding the asset boundary to ensure consistent application and auditing.

The SDT has made modifications in the second posting of the requirement. The requirement has been modified to address inbound and outbound communications only with the low impact BES Cyber System. The reference to the asset boundary has been removed. The Guidelines and Technical Basis have been modified to provide more clarity, and examples, around the electronic access controls that can be used and how they may be implemented in a manner that meets the operational needs of the entity.

Definition of LERC

Stakeholders commented that the proposed definition of LERC creates more ambiguity and will lead to all substations containing low impact BES Cyber Assets will have LERC.

The SDT has made modifications in the second posting of the requirement. In response to these concerns, the SDT has removed the definition of LERC and instead has chosen to clearly state the security objective for electronic access controls and define criteria for when they must be implemented. These criteria address the concern that all substations could be identified as having LERC even when those communications are not used for BES purposes.

Demonstration of Compliance

Stakeholders commented that it was unclear how to document LERC electronic access controls, especially for physically isolated and logically isolated systems. One commenter questioned whether a detailed network drawing is required; whether there is a need to label devices and ports for identification during an audit; if the documentation can be a list and would a list have to identify each LERC individually; etc. One commenter suggested an asset list and/or diagrams as the best way to identify its low impact BES Cyber Systems and possibly confirm electronic access control applied. Lastly, the same commenter was concerned that Section 3 would not show the low impact BES Cyber Systems the electronic access control was implemented on.

Physically and logically isolated systems no longer require the implementation of electronic access control. Attachment 2 of CIP-003-7 contains examples of evidence that can be used to demonstrate compliance where electronic access controls are required.

Exclusion Language

A single stakeholder representing a number of its members raised concern about the use of "non-Control Center BES" in the current LERC definition. Specifically, that there may be scenarios where a Remedial Action Scheme (RAS) could have components in a low impact control center that requires sub-second communication capability. This may result in unintended consequences to reliability and/or compliance.

The SDT references the resulting modifications in the second posting of the requirement and does not believe that an exclusion provision will necessarily have a negative impact to reliability and/or compliance.

Expansion of Scope

Several stakeholders noted that the proposed change in language expands the scope but does not reduce the ambiguity as required by Order No. 822. The ability to demonstrate compliance is limited and leads to varying levels of sophistication for control. Also, that the proposed language should be revised to clarify that the scope does not apply to non-BES Cyber Assets. For example, controls would be implemented to secure LERC even though there is no LERC "connection" to a low impact BES Cyber System. Therefore, Cyber Assets that would normally be considered out-of-scope could inadvertently be included in this case.

The SDT has made revisions to address inbound and outbound communications only with the low impact BES Cyber System. Flexibility refers to the various reference models that can be implemented to achieve the objective of the electronic access control.

Guidelines and Technical Basis

Stakeholders suggested modifications to the Guidelines and Technical Basis. One comment concerns the use of an "air gap" as an electronic access control mechanism citing that an air gap is overly burdensome and may be difficult to document for compliance. Another commenter suggested revising the sentence, "[t]he electronic access control depicted in this reference model may not meet the security objective for controlling device-to-device communication across the LERC depending on the specific system configuration in place" to include a specific example that would be compliant versus one that would be non-compliant. Additionally, two stakeholders support the SDT approach with one agreeing that the identification of the proper boundary for the low-impact facility is a much more straight-forward process than attempting to differentiate between direct and indirect access. The commenter did not find any gaps in the materials, but would hope that the drafting team captures any new relevant examples that may arise during the review of CIP-003-7.

Based on comments received, the SDT has further modified the guidelines to provide more clarity around the electronic access controls that can be used and how they may be implemented.

Use of "Necessary"

Stakeholders commented about the use of "necessary" being used in the requirement and suggested alternatives.

The SDT has modified the requirement to address only necessary inbound and outbound communications with the low impact BES Cyber System.

Miscellaneous Comments

Define electronic access control – A single comment recommended the SDT define the term "electronic access controls" (and provide the examples as part of the definition).

The SDT contends that the common understanding of electronic access controls as well as the stated security objective and supporting Guidelines and Technical Basis provide for a comprehensive understanding of the controls that may be implemented.

Examples in Requirement – A single commenter suggested adding examples of controls in Attachment 1 rather than as part of the examples of evidence in Attachment 2. Inclusion of examples, such as those listed in Attachment 2, will ensure a secure method to protect LERC and reduce risk to the BES.

The SDT contends that examples of implementation are best suited for Measures or the Guidelines and Technical Basis. The requirement language is targeted to the security objective.

FERC NOI – A single commenter suggested addressing concerns identified for any LERC that passes information to any high or medium impact Electronic Security Perimeter (ESP) utilizing a transmission path that is not exclusively dedicated to communications for use by an Entity or between Entities is not permitted (or at least must be identified so that the risk is recognized).

The SDT will be addressing communications between control centers as part of the project scope, but not in this draft.

Question 4: Measure Language

Summary Response

4. Measure M2: The SDT revised the complementary language of CIP-003-6, Attachment 2, Sections 2 and 3 to make the evidential language of the Measure consistent with the revised requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal

Suggested Language and Clarifying Revisions

Several commenters suggested both substantive and non-substantive language changes. The SDT has carefully considered each such comment and has implemented revisions to adjust and further clarify the language where needed.

One commenter noted that, for each asset or group of assets that contain LERC, documentation showing that communication to Low Impact BES Cyber System is confined to only that which the Responsible Entity deems necessary. The commenter also suggested examples of this documentation could include representative diagrams or lists of the implemented electronic access controls (e.g., restricting IP addresses, ports, or services; authenticating users, air-gapping networks; terminating routable protocol sessions on a non-BES Cyber Asset; implementing unidirectional gateways). Another commenter raised an issue with the language of Attachment 2, Section 3, Paragraph 1, particularly noting comma placement, and proposing alternative language.

The SDT revised the language to address concerns and clarify the intent of the Attachment.

Requests to Provide Specific Examples

More than one commenter suggested the SDT provide specific examples of compliance measures in cases where LERC or dial-up connectivity is not present.

The SDT believes that the intent of the measures is to provide examples of evidence to demonstrate compliance with the requirements.

Several commenters expressed concerns related to the Reference Models and Attachment 2.

At least one commenter suggested that the proposed LERC term may create a condition whereby non-BES Cyber Assets will be considered BES Cyber Assets, subjecting those assets to CIP-002-5.1 compliance. The commenter noted that, while such inventories are not explicit in CIP-003-6, Attachment 2, Sections 2 and 3, it may be perceived that an inventory of all low impact BES Cyber Assets, including determination, is now required.

The SDT has revised the Requirements and adjusted measures for clarification.

One commenter stated that proposed Attachment 2, Section 3, may be unclear as to what extent air-gapping as an electronic access control is acceptable.

The SDT has removed the above-mentioned content from Attachment 2, and provided clarification in the Guidance and Technical Basis document.

More than one commenter suggested the SDT add further information for clarity related to the intended use, and documentation required for, Reference Model 7 and Reference Model 8. At least one of those commenters also raised several issues related to the language in Attachment 2 Section 3: documentation, particularly the following language: “termination routable protocol sessions on a non-BES Cyber Asset,” raising the issue that this could facilitate a “pivot attack” if the non-BES Cyber Asset it compromised. Similarly, another commenter expressed concern that the allowance of terminating routable protocol sessions on a non-BES Cyber Asset could, depending on the configuration of the intermediate system, enable a pivot attack.

The SDT adjusted the Reference Models to reflect the revised Requirement language and provided additional clarity on the examples raised by the commenters.

Concerns with Reference Models and Attachment

At least one commenter stated that the language of CIP-003-6, Attachment 2, Section 3-1 does not properly restrict the applicability to the Low Impact BES Cyber Systems within an asset.

One commenter requested the SDT clarify whether the addition of the language In Attachment 2, Section 3, providing examples of evidence "such as representative diagrams or lists of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; authenticating users; air-gapping networks; terminating routable protocol sessions on a non-BES Cyber Asset; implementing unidirectional gateways)" is intended to revise Requirement R2.

The SDT has revised the requirements, adjusted measures for clarification, and added references to the Attachments for what is represented in each to add clarity.

General Comments

One commenter stated that the SDT provide encouragement to entities to have an inventory of their low impact BES Cyber Systems. A second commenter also raised this concern, and added that the concepts of LERC and asset boundary create compliance violation uncertainty.

The SDT disagrees that entities should be encouraged to maintain inventory of their low impact BES Cyber Systems, rather, it is the position of the SDT that language revisions to proposed Requirement R2 adequately address this issue.

One commenter asserted that they support the revised measure, and stated that it appears that a single representative diagram could be utilized as substantiating evidence for several BES assets that share a common configuration. The commenter referred to the following statement as support for this conclusion: “Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to: 1. Documentation, such as representative diagrams or lists of implemented electronic access controls. . .,” noting that the use of a single representative diagram as substantiating evidence for several assets that share a common configuration could relieve entities of added compliance burden related to documenting LERC under the proposed definition. The commenter further stated that they support the new definition and this approach to demonstrate compliance.

Question 5: Guidelines and Technical Basis

Summary Response

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides example diagrams that illustrate various electronic access controls at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

Reference Models

Overall, the SDT received support for including the reference models in the Guidelines and Technical Basis section of the standard. The SDT received requests for additional reference models including Dial-up Connectivity, Wireless, SONET, MPLS, and reference models for which electronic access controls are not required. The SDT also received requests to include the data flow depiction in all of the reference models.

The SDT appreciates the support for the inclusion of reference models with the standard. The SDT chose not to include a reference model for Dial-Up Connectivity as the SDT did not make material changes to CIP-003-6 Attachment 1, Section 3.2 regarding Dial-Up Connectivity. The SDT did add a reference model for SONET which included discussion about other wide area transport methods and for reference models where electronic access controls are not required. The SDT did not add a reference model for wireless connectivity as the team generally understands the concepts for wireless connectivity and wired connectivity to be the same.

Additionally, the SDT considers the issues raised around wireless connectivity to be based upon the concepts of air-gapping as an electronic access control and the identification of a defined asset boundary. As these two elements were removed in the revised draft, the SDT determined that a diagram depicting wireless connectivity was not necessary. Finally, the SDT added arrows indicating the data flow path to all diagrams as requested.

Suggestions for Language Clarity

The SDT received numerous comments on language in the Guidelines and Technical Basis that was unclear, contained grammatical errors, or where commenters identified that terms were improperly capitalized. In particular, comments indicated confusion around the shorthand of “BES Asset” to reference an “asset containing low impact BES Cyber System(s)” and its use in the reference models conjoined with the concept of “asset boundary.”

The SDT has attempted to correct all of the issues raised by commenters including removing use of the term “BES Asset” as shorthand for “asset containing low impact BES Cyber System(s).” The concept of asset boundary has been removed from the standard in this draft, thus resolving issues with its use. Some labels included in the reference models are capitalized consistent with title case, but this does not indicate that the term is a term defined in the NERC glossary. An example of this

title case includes the legend for all diagrams which indicates the line format for "Non-routable Protocol."

Implementing Physical Access Controls

The SDT received some comments addressing areas of the standard and Guidelines and Technical Basis that were not modified with these revisions, such as comments on what methods are acceptable approaches for implementing physical access controls.

The work of this SDT does not change the intent or meaning of unmodified requirement language or Guidelines and Technical Basis language. As such, modifications to the Guidelines and Technical Basis were only made consistent with the modifications to the requirement language made by this SDT.

Air-Gapping

The SDT received comments regarding the question about the Guidelines and Technical Basis about the scope of the requirement language and whether the inclusion of "air-gapping" as an acceptable electronic access control implies that electronic access controls for communications that are used exclusively for non-BES applications must be identified and evaluated.

The modifications to the requirements language with the introduction of criteria that communications must be "between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System" generally resolves this issue. To further clarify the intent of the requirement, the SDT added language to the Guidelines and Technical Basis which states: "any communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), does not require evaluation for electronic access controls."

Asset Boundary Clarification

The SDT received many comments about the lack of clarity around the concept of asset boundary which was used in the first draft of CIP-003-7. While the original draft included some language in the Guidelines and Technical Basis, commenters had numerous questions indicating that the concept of assent boundary was not clear.

The SDT addressed the comments regarding the asset boundary by removing the "asset boundary" in this draft. The SDT reiterated in the requirement language as well as in the Guidelines and Technical Basis that the requirement is applicable to the assets identified pursuant to CIP-002 as containing low impact BES Cyber System(s). The Guidelines and Technical Basis further clarifies the new criteria introduced in the revised requirement language including a reference model discussing "indirect access" as meeting the criteria for communications "between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber System(s)."

The revised Guidelines and Technical Basis also explains that Responsible Entities have flexibility in identifying an approach to determining whether routable protocol communications enters or leaves

an asset containing low impact BES Cyber System(s) and introduces two methods for performing this evaluation.

Miscellaneous Comments

The SDT also received numerous comments asking the SDT to make changes to the Guidelines and Technical Basis consistent with modifications that they suggested in their response to the questions about the requirement language itself.

SDT has considered all of the input and made changes to the Guidelines and Technical Basis consistent with the modifications to the requirement language and informed by the feedback received from stakeholders.

Question 6: Implementation Plan

Summary Response

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) for the revisions made to Sections 2 and 3 of Attachment 2 in CIP-003, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is nine (9) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If not, please provide the basis for your disagreement and an alternate proposal.

Expansion of Scope and Volume of Assets

Stakeholders raised concerns about the time needed to implement CIP-003-7 due to the expansion of scope created by the LERC definition revisions. To implement, stakeholders saw the approach as requiring entities to start over with their evaluation of all assets containing low impact BES Cyber Systems to determine and possibly inventory the instances of LERC whether connected to a BCS or not. The timeline was seen as too tight to manage the large volume of assets that fall into the low category. Stakeholders further pointed out that the timeline did not recognize the time for identifying acceptable solutions, procuring new infrastructure, and installing these modifications, and the budget cycle that entities must also manage for such undertakings.

The drafting team responded to the concerns about the LERC definition revisions by changing the approach to address the FERC directive concerning LERC. The SDT proposes retiring the LERC definition (and the LEAP definition) and incorporating the LERC concepts within the requirement language. This approach returns the focus of the requirements onto controlling electronic access to BES Cyber Systems and results in removal of the step to identify LERC.

Overlap of -6 and -7 / Duplication and Budget Challenges

Stakeholders noted concerns that CIP-003-6 currently has a September 1, 2018 deadline and that the revisions underway present a possible duplication of effort if entities have to implement -6 and then change their programs to implement -7. Stakeholders saw the proposed LERC revision as a substantial rewrite which would warrant starting over to implement once approved. Even without dramatic change to the definition and requirements, since the implementation work for -6 is currently underway, entities want to see that a revised version leverages the current work underway for -6 to minimize duplicative cost and effort. Many acknowledged that the SDT may not be able to suspend the implementation deadline for -6 to replace with -7; though, stakeholders requested that the issue be considered and potentially raised with FERC. There were suggestions to defer CIP-003-6, Attachment 1, Section 2 and 3 or begin enforcement on the effective date of version 7.

In response to comments, the SDT adjusted the approach to the revisions. The SDT proposed retiring the LERC definition (and the LEAP definition) and incorporating the LERC concepts within the requirement language. The SDT intends for this approach to be more consistent with

implementation work currently underway. However, the SDT recognizes that entities may need to adjust their implementation when -7 is approved and avoiding duplication of work is most desirable. The SDT does not have authority to change the deadlines for -6, but the revised implementation plan clarifies the intent for CIP-003-7 to replace the deadlines for CIP-003-6, Attachment 1, Sections 2 and 3.

Other Coming Changes

A few stakeholders appealed for consideration of the many implementation demands being placed on entities including the SDT work on Transient Cyber Assets (TCA) at lows.

While this posting of CIP-003-7 addressed the LERC directive from Order 822, the SDT has also drafted proposed changes in response to Transient Cyber Assets directive also applicable to assets containing Low Impact BES Cyber System. The SDT is working to post those proposed revisions in an effort to provide stakeholders with one set of revisions applicable to assets containing low impact BCSs and to minimize the recurring revisions.

Single Date Approach

Stakeholders appreciated the effort to align the coming effective dates and setting a single compliance date.

The SDT continues to propose a single date for CIP-003-7, Sections 2 and 3 to simplify the management of multiple dates during implementation and maintain consistency with the format of implementing version 6.

More Time Needed

Several stakeholders proposed a number of alternative timelines from 12 months to 32 months with a few entities stating that the proposal presented too many issue in need of clarification before an accurate timeline could be proposed.

The SDT is proposing 12 months because the new approach (i.e., incorporating the LERC and LEAP concepts in the requirements) is more consistent with the currently approved CIP-003-6 approach and removes the language in the initial proposal that raised stakeholder concerns over expansion of scope. The SDT selected 12 months to allow entities to adjust their CIP-003 implementation to reflect the revised language and to implement across the multitude of assets that are in scope under CIP-003.

Miscellaneous Comments

One commenter asked that the implications for changes in implementing CIP-003, R1.2.3 be reviewed. The SDT reviewed R1.2.3 and has included clarifying language in the Implementation Plan.

One commenter supported the proposed implementation timing, but requested further justification for the time allotted. One commenter supported 9 months, but questioned the justification for the

period. The SDT is supporting a 12 month implementation to accommodate the number of locations brought into scope and the possible variations associated with the requirement revisions.

Another stakeholder requested using a separate standard to house all the requirements applicable to lows (i.e. CIP-012). Another commenter suggested placing all the requirements associated with lows into a singles standard. The majority of stakeholders support an approach within CIP-003-7. EEI, Mid- American and TVA offered alternate approaches for the team to consider. The SDT considered other suggested alternate approaches to address the issues raised by commenters. The SDT has selected an approach that appears to address the majority of concerns raised by commenters.

One commenter inquired in regards to how Regional Entities conduct audits during the period identified within the Implementation Plan?

Since, auditing is not within the purview of the SDT, this question will need to be addressed to the Regional Entities and NERC.

Question 7: Additional Comments

Summary Response

7. If you have additional comments on the proposed revisions to address the FERC directive regarding the LERC definition that you have not provided in response to the questions above, please provide them here.

Beyond the Scope of FERC Order

Commenters raised questions regarding the proposed changes to LERC expand the amount of items included, and do not directly address the ambiguity of the term "direct", as directed by the Commission. A proposal was provided that the SDT retain LEAP and address the Commission's instruction to "provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition."

In addressing the security objective related to "direct", it became clear to the SDT that the requirement could be improved to remove ambiguity and clearly identify the necessary controls to protect low impact BES Cyber Systems. Please see the resulting modifications in the second posting of the requirement.

Language in the Requirement

Concerns regarding communications that pass through an asset boundary were expressed. One concern was that communications will pass through the asset boundary but will not terminate on anything inside the boundary (i.e. fiber cable passing through). Another concern was about identifying asset boundaries for shared facilities because we are under the impression that both entities have to account for all communications. In the event that one of the entities' is not a NERC registered entity, they were concerned that they would need to account for all communication paths including those that have nothing to do with the BES. They recommend limiting the scope only to those paths that are used for BES communications or connect to BES Cyber Assets.

Please see the resulting modifications in the second posting of the requirement. The requirement has been modified to address inbound and outbound communications only with the low impact BES Cyber System.

One commenter pointed out that the justification provided for the approach the SDT took adds an increased compliance burden without added benefit to the security of BES, or any assurance that entities will not be asked for a list of BES Cyber Assets at Low Impact BES Assets.

Please see the resulting modifications in the second posting of the requirement. The requirement has been modified to address inbound and outbound communications only with the low impact BES Cyber System, regardless of criticality of the communication. CIP-002-5.1 does not require a list of low impact BES Cyber Systems.

One commenter stated his/her belief that low impact BCAs should be within an Electronic Security Perimeter (ESP). They referenced the purpose statement in CIP-005-5, which reads, "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."

The SDT contends that requiring an ESP for low impact BES Cyber System may not be practical in implementation based on the diversity of situations. The security objective of the requirement accomplishes the basic premise of and ESP but also allows for other implementations that may be more appropriate to the Entity.

Commenters expressed that there is a significant gap in the revised requirements and accompanying definition of Low Impact External Routable Communication (LERC). Unlike the requirements for High and Medium Impact BES Cyber Systems, there is no concept of a Protected Cyber Asset due to the absence of an Electronic Security Perimeter. While the requirement for electronic access controls would conceivably protect non-BES Cyber Assets connected to the same routable network, there is no requirement to protect such Cyber Assets from unauthorized physical access. The requirement is to control physical access, based on need as determined by the Responsible Entity, to the asset or the locations of the low impact BES Cyber Systems within the asset. To the extent that non-BES Cyber Assets are collocated with Low Impact BES Cyber Systems, physical protections will be afforded. However, with the provision in the "Determining Asset Boundary" section of the Guidelines and Technical Basis to expand the "asset boundary" beyond the "fence line," coupled with the option to control physical access only to the locations of the Low Impact BES Cyber Systems as opposed to protecting the asset in total, non-BES Cyber Assets could reside within the defined asset boundary but not within the physical protection zones permitted by the Standard. This gap introduces an unacceptable risk of attack that would allow the malicious actor ready access to the unprotected Cyber Assets and thus to the connected network, bypassing the electronic access controls designed to protect the Low Impact BES Cyber Systems.

The requirement under section 2 and section 3 of Attachment 1 are aligned with the protection of the low impact BES Cyber System. The SDT contends that proper implementation of the physical access controls and electronic access controls provide sufficient protection of the BES Cyber System from unauthorized access by properly securing and effectively isolating the BES Cyber System.

Guidelines and Technical Basis

An entity noticed many comments regarding the "asset boundary" part of the proposed definition is causing some concern with Registered Entities (Entity), with most of those comments related to what is the boundary and could there be differences of opinion on what is the boundary at audit time between the Entity and Audit Teams. They felt the information in the Guidance and Technical Basis (GTB) section of proposed CIP-003-7 has sufficient information to indicate what could be the "asset boundary" and using a practical approach in determining the boundary there should be no question as long as the Entity clearly documents how they arrived at the identification of the boundary. They also believed that it would be beneficial if the GTB text provided some guidance on

how the boundary could be documented to reduce concerns that their determination of the boundary would be questioned by Audit Teams.

Please see the resulting modifications in the second posting of the requirement. The Guidelines and Technical Basis have been modified to provide more clarity around the electronic access controls that can be used and how they may be implemented.

Some of the Reference Models may be incorrect in the labelling of non-routable versus routable protocols (e.g. Reference Model 1 left-hand side).

The left side of Reference Model 1 is to show that routable communication can take place between the BES Cyber Systems and the communication is protected from other Cyber Assets by the air gap. The Guidelines and Technical Basis have been modified to provide more clarity around the electronic access controls that can be used and how they may be implemented.

One entity stated that they had repeatedly encountered the argument that data traffic passed over Layer 2 networks is not routable communication. There is a significant difference between routable communications and routing networks. Layer 3 (routable) traffic encapsulated with Layer 2 headers for transmission over a Layer 2 network segment does not result in non-routable communications. It is the presence of network (not MAC) addresses in the Layer 3 header of the data packet that makes the communication routable. This should be clarified in the Guidelines and Technical Basis section of CIP-003-7, or the term should become a defined term in the NERC Glossary.

The SDT contends that the common understanding of routable protocols and routable communication are sufficient in addressing the requirement language. The reference models in the Standard provide clear examples for implementation of acceptable access controls.

Implementation Plan

The current effective date of CIP-003 R1.2.3 requiring a Cyber Security Plan for "Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-Up Connectivity" is April 1, 2017. One commenter believes that the Cyber Security Plans for Low Impact BCS in R1.2.3 is dependent upon the definition of LERC and the requirements for CIP-003, Attachment 1, Section 2 and 3 that are currently in flux. They recommended that the effective date for CIP-003 R1.2 to align with the effective dates for CIP-003-7, Attachment 1, Section 2 and Section 3.

The SDT contends that entities should proceed with the required implementation dates for the approved standard, CIP-003-6 except where the proposed CIP-003-7 implementation plan notes. This includes implementation of the policy required under CIP-003-6 Requirement 1.2 which is foundational to defining the require security plan under Attachment 1.

There was concern that the Implementation Plan makes no mention of current efforts to address LEAPs. What guidance is available for documenting and testing LEAPs? How will Regional Entities conduct audits during the period identified within the Implementation Plan? What actions should Registered Entities follow during this period?

The SDT contends that Entities should proceed with the required implementation dates for the approved standard, CIP-003-6. The security objective under CIP-003-7 leverages the concept of LEAP as a security control. This should reduce any negative implementation impact on Entities. Auditing practices during the transition will need to be addressed by the ERO.

One commenter noted that the language in the definitions and CIP-003-7 currently out for vote is a substantial rewrite of the requirements as approved by FERC. Entities cannot afford to wait to begin implementation until a revised standard is approved by FERC, meaning that any approved version that does not allow an entity to leverage work efforts already completed in alignment with the current FERC approved standard would lead to duplicative effort and costs. Any attempt to compress the overall timeline for implementation could result in a negative impact to the reliability of the bulk electric system.

The SDT proposed an implementation timeframe noted in the Implementation Plan as sufficient to achieve compliance with the requirements.

The decision to do away with LEAP, though understandable from an economic standpoint, would have profound implications on access control implementation and enforcement.

The SDT proposed an implementation timeframe noted in the Implementation Plan as sufficient to achieve compliance with the requirements.

Miscellaneous Comments

Some commenters noted that the SDT should remove the Interchange Coordinator and Interchange Authority functions from the list of applicable functional entities, as these functions were retired in 2015.

The SDT believes that this comment is not relevant to the modifications made in response to the LERC issue.

One stakeholder commented that CIP-002 should be split into two separate standards. R1, R1.1, and R1.2 are planning functions and require a great deal of hair splitting because the deliverable is not clearly defined in the standard. R1.3 and the rest of the standard is about cyber security. Planning engineers don't typically know cyber security and cyber security people don't typically know transmission systems. No one wants to take responsibility for a standard and analysis that they have no other need to know. Rewriting the standard to separate R1, R1.1, & R1.2 from R1.3 and R2 would streamline the compliance effort tremendously.

The SDT notes that modifications of this nature to CIP-002-5.1 are not within the scope of the currently approved SAR.

One commenter believed the SDT should define "asset." Based on the "Low Impact" criteria in CIP-002, they believe the SDT should define the term "Asset" as follows:

- Control Centers and backup Control Centers

- Transmission stations and substations
- generation resources
- Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements
- Special Protection Systems that support the reliable operation of the Bulk Electric System

For Distribution Providers, Protection Systems specified in Applicability Section 4.2.1 of CIP-002.

Commenters expressed concern that if the term is being used to specifically reference something that is called out in the standards and requires controls, then it should be formally defined.

The SDT contends that CIP-002-5.1 provides the necessary information for an Entity to identify their assets without creating a defined term.

One entity suggested that “routable protocol(s)” and/or “routable communication(s)” should be defined in the NERC Glossary of Terms and examples given within the definition.

The SDT contends that the common understanding of routable protocols and routable communication are sufficient in addressing the requirement language.

Commenters noted that from a formatting perspective, it would be helpful to use a consistent approach to paragraph and section numbering. There is a mixture of numbers, bullets, and no numbering at all. A consistent number format is very helpful when trying to reference parts or sections of the document in attachments 1 & 2.

The SDT contends that the formats for numbering and bullets are as required. A bulleted list denotes items that are options for the Entity and utilize the distinguisher of “or”. A numbered list denotes items that are required by the Entity and utilize the distinguisher of “and”.

Several entities expressed concerns regarding the ongoing modification to the low impact BES Cyber System requirements, and that the SDT may want to consider removing the low impact requirements from CIP-003 and create a new standard.

The SDT previously considered separating Low Impact BES Cyber Systems from CIP-003 and creating a new standard; however, many entities expressed a preference for the requirements in question to remain in CIP-003 and approved CIP-003-6 as the standard to hold the requirements.

Several entities requested that NERC place items related to electronic boundary protection in CIP-005, not CIP-003. The same should apply to physical protections of low. Low requirements should be placed in the standard that closely matches the medium requirements. Transient devices should be in their own standard (i.e., CIP-012). The CIP-003 standard should not be a parking lot for newly developed requirements.

Based on prior industry support of having all low impact requirements in a single standard, the SDT has determined that CIP-003 is still the proper location for the requirements.

Commenters expressed that transient LERC(s) should be addressed in this Standard or in response to the FERC directive to address Transient Cyber Assets at Low Impact. The Standard should address dynamic connectivity into low impact substations. This may include Transient Cyber Assets, mobile substations, intermittent session based communication, and cellular network connections.

Please see the resulting modifications in the second posting of the requirement. The requirement has been modified to address inbound and outbound communications only with the low impact BES Cyber System. Additionally, there is a posting for Transient Cyber Assets related to low impact BES Cyber Systems.

One commenter noted that these standards are still ambiguous and would therefore be subjective to the auditor.

The SDT contends that in addressing the security objective related to "direct," the SDT addressed the ambiguity and clarified the requirement to identify the necessary controls to protect low impact BES Cyber Systems. Please see the resulting modifications in the second posting of the requirement.

Stakeholders also commented that although not directly within the scope of this project, the SDT is encouraged to review the Violation Time Horizons set forth in the Standard. From an Enforcement perspective, Violation Time Horizons have a significant impact on the ultimate penalty determination. As such, the SDT may wish to consider the current Operations Planning time horizon set forth in the Standard and articulate a basis for this conclusion.

Modifications to the Time Horizon are not within the scope of the currently approved SAR.

Regarding non-binding VRF/VSL poll, a commenter noted that it is inconsistent with the risk based methodology for an entity that updates its high and medium impact cyber security policy after 15 months but prior to 16 months to have a lower VSL, but the same entity that fails to update the low impact cyber security policy in 15-16 months to have a medium VSL.

Modifications to Requirement 1 are not within the scope of the currently approved SAR.

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.

Description of Current Draft

This draft of CIP-003-7 is addressing the directive issued by the Federal Energy Regulatory Commission (Commission) in paragraph 73 of Order No. 822 which reads:

> [T]he Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule approving revisions to the cybersecurity Critical Infrastructure Protection (CIP) standards.

In this revision, the SDT revised Sections 2 and 3 of Attachments 1 and 2 in CIP-003-7 and removed the terms *Low Impact External Routable Connectivity* (LERC) and *Low Impact BES Cyber System Electronic Access Point* (LEAP). The modifications incorporate concepts and select language from the LERC definition into Attachment 1, Section 3 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). The SDT simplified Section 3 of Attachment 1 to require the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the exclusion language (previously in the definition of LERC) contained in (iii) which reads: "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The defined term LEAP is no longer necessary because the SDT changed the requirement from requiring a LEAP to requiring electronic access controls. Additionally, since the SDT is removing the term LERC, the exclusion language that was previously in the definition of LERC was integrated into the Attachment 1, Section 3.1 requirement.

Because the proposed modifications to Reliability CIP-003-7 eliminate the need for the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP), NERC is requesting these terms be retired in the associated Implementation Plan.

Additionally, the SDT:

- revised the associated Lower, Moderate, and High VSLs for Requirement R2 to complement the requirement revisions;
- corrected a mistake in the Severe VSL for Requirement R2;
- made non-substantive changes to the Moderate and High VSLs for Requirement R2 to align with the order of the requirement;
- removed repetitive text from Requirement R1, Part 1.2.3 to make it consistent with Parts 1.2.1 and 1.2.2;
- updated the Guidelines and Technical Basis section of the standard to reflect the revisions made to the Attachments; and
- made non-substantive errata changes throughout the standard such as replacing "ES-ISAC" with "E-ISAC".

Completed Actions	Date
Standard Authorization Request (SAR) approved	July 20, 2016
Draft 1 of CIP-003-7 posted for formal comment and initial ballot	July 21 – September 6, 2016
Draft 2 of CIP-003-7 posted for formal comment and additional ballot	October 21 – December 5, 2016

Anticipated Actions	Date
10-day final ballot	January, 2017
NERC Board of Trustees (BOT) adoption	February, 2017
Petition filed with FERC	March, 2017

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-7

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 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 SPS or RAS where the SPS or 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-003-7:

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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3 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.

4.2.3.4 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-003-7.

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single

cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls; and

1.2.4. Cyber Security Incident response

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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate

implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans	containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented	failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2)	its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification,	The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(E-ISAC) according to Requirement R2, Attachment 1, Section 4.		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but	The Responsible Entity has used delegated authority for actions where allowed by the CIP

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specific actions delegated, but 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. (R4)	specific actions delegated, but 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. (R4)	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. (R4)	Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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.	

Version	Date	Action	Change Tracking
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 devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees.	Revised to address FERC Order 822 directive regarding definition of LERC.

Attachment 1

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

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

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

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

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security control objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition…within one year of the effective date of this Final Rule.

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the exclusion language (previously in the definition of LERC) contained in (iii) which reads: "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The

focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

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

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

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

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and,

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Attachment 2

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

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

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

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

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

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

1. Documentation, such as representative diagrams or lists of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; implementing unidirectional gateways) showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices; and
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The Responsible Entity is not required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls outlined in Section 2, this can be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with

locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The requirement does not obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, Responsible Entities are to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities

should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, any communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), does not require evaluation for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

In order for Responsible Entities to determine whether electronic access controls need to be implemented, the Responsible Entity needs to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that use a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach to making this evaluation. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the Responsible Entity documents and implements its chosen electronic access control(s). The control(s) must allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. The Responsible Entity must be able to explain the reasons for the electronic access permitted. The reasoning for the "necessary" inbound and outbound electronic access controls can be documented within the Responsible Entity's cyber security plan(s) or other policies or procedures associated with the electronic access controls.

Concept Diagrams

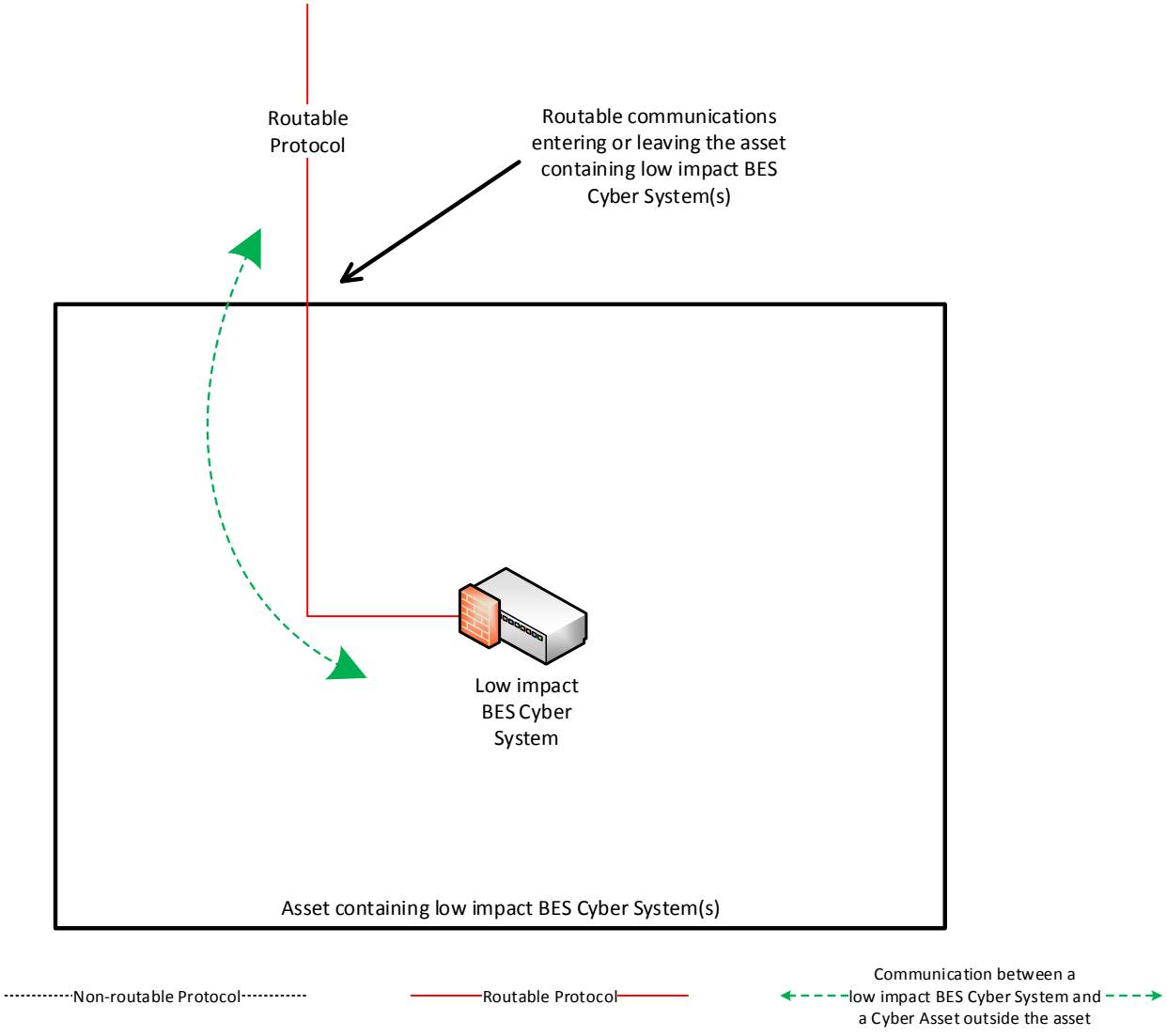
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset must be met.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

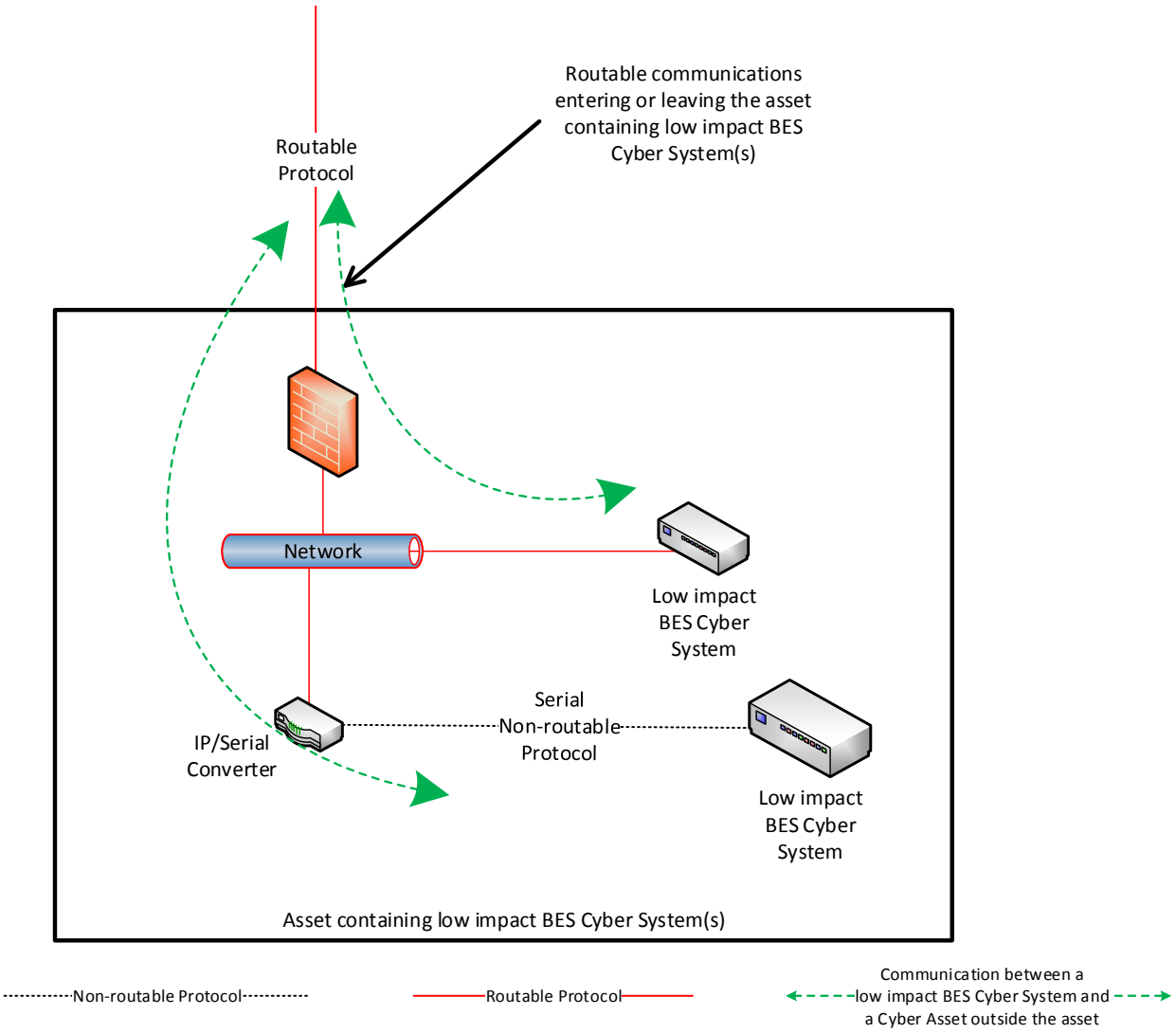
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound routable protocol access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary. Responsible Entities may further restrict electronic access using ports and services based on the capability of the electronic access control, low impact BES Cyber System, application, etc.



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

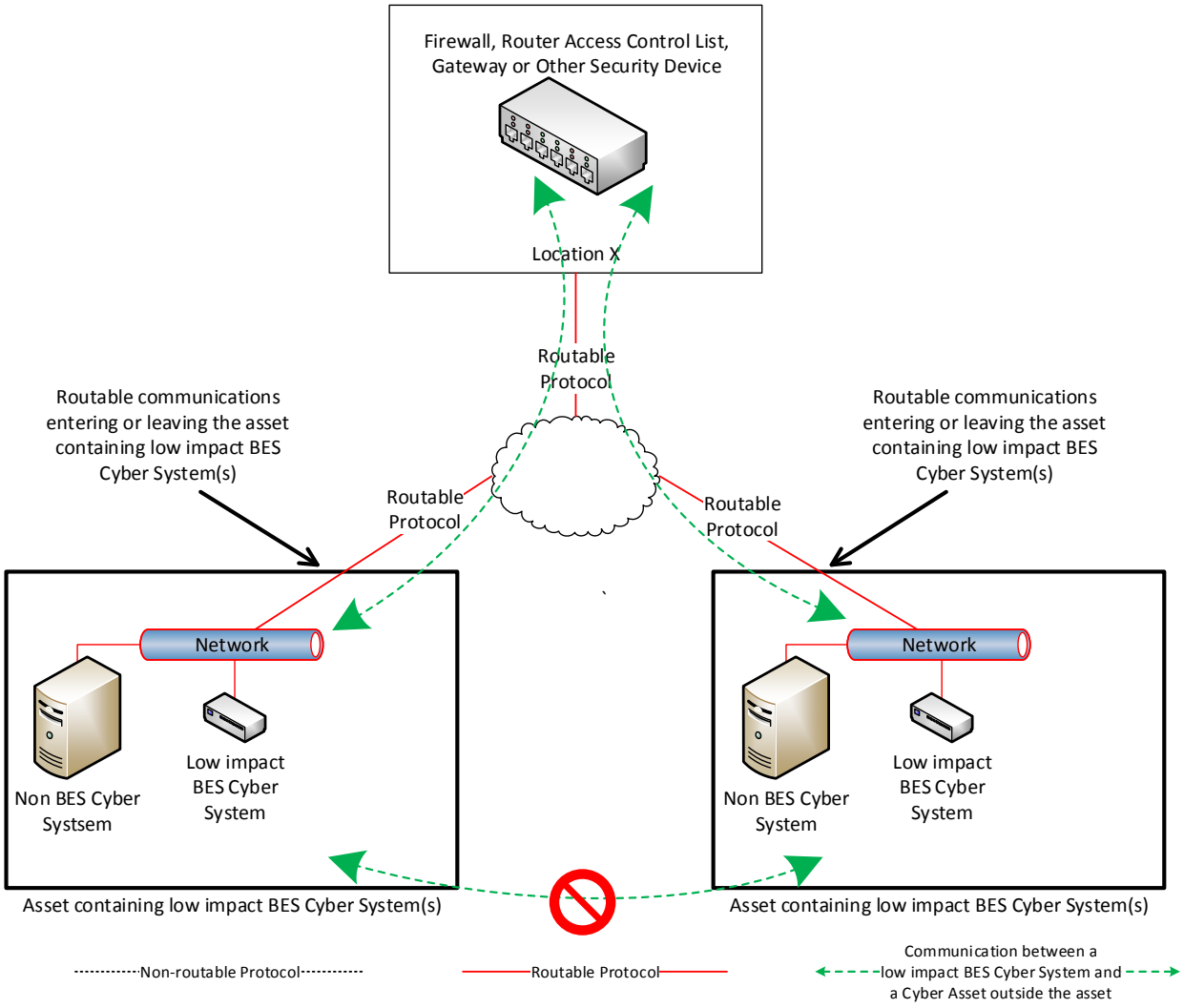
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary. Responsible Entities may further restrict electronic access using ports and services based on the capability of the electronic access control, low impact BES Cyber System, application, etc.



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

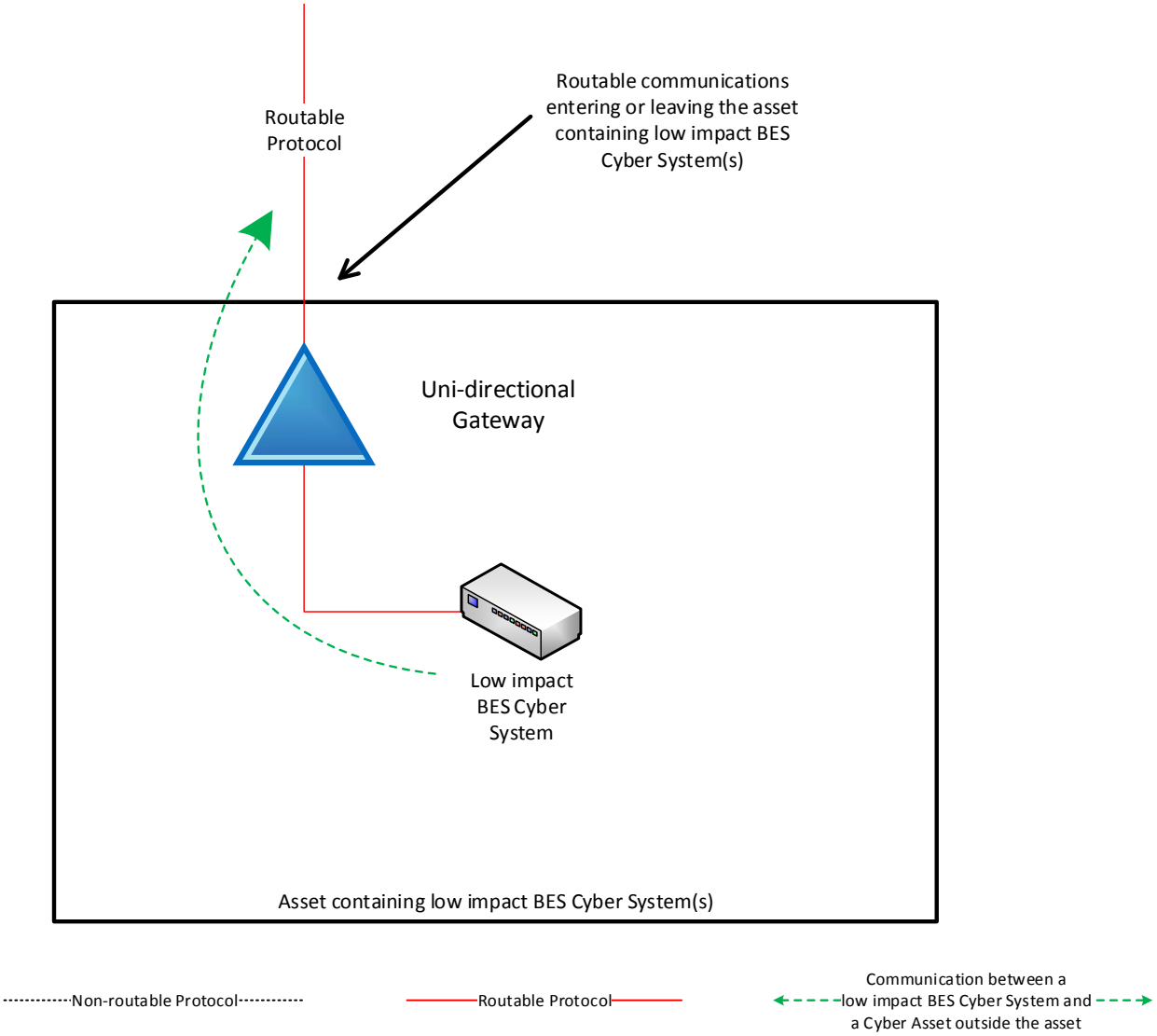
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary. Responsible Entities can further restrict electronic access using ports and services based on the capability of the electronic access control, low impact BES Cyber System, application, etc.



Reference Model 3

Reference Model 4 – Uni-directional Gateway

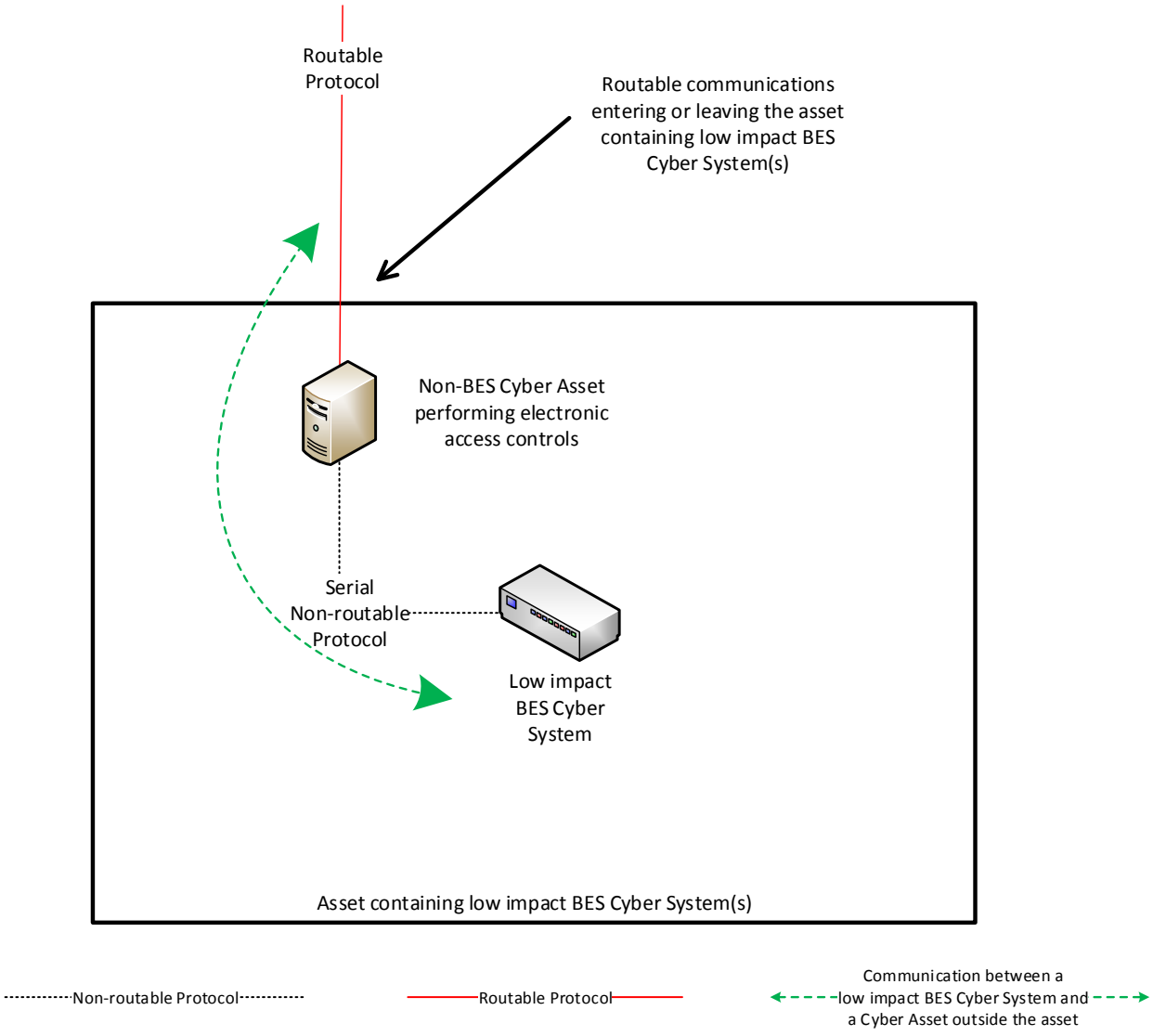
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

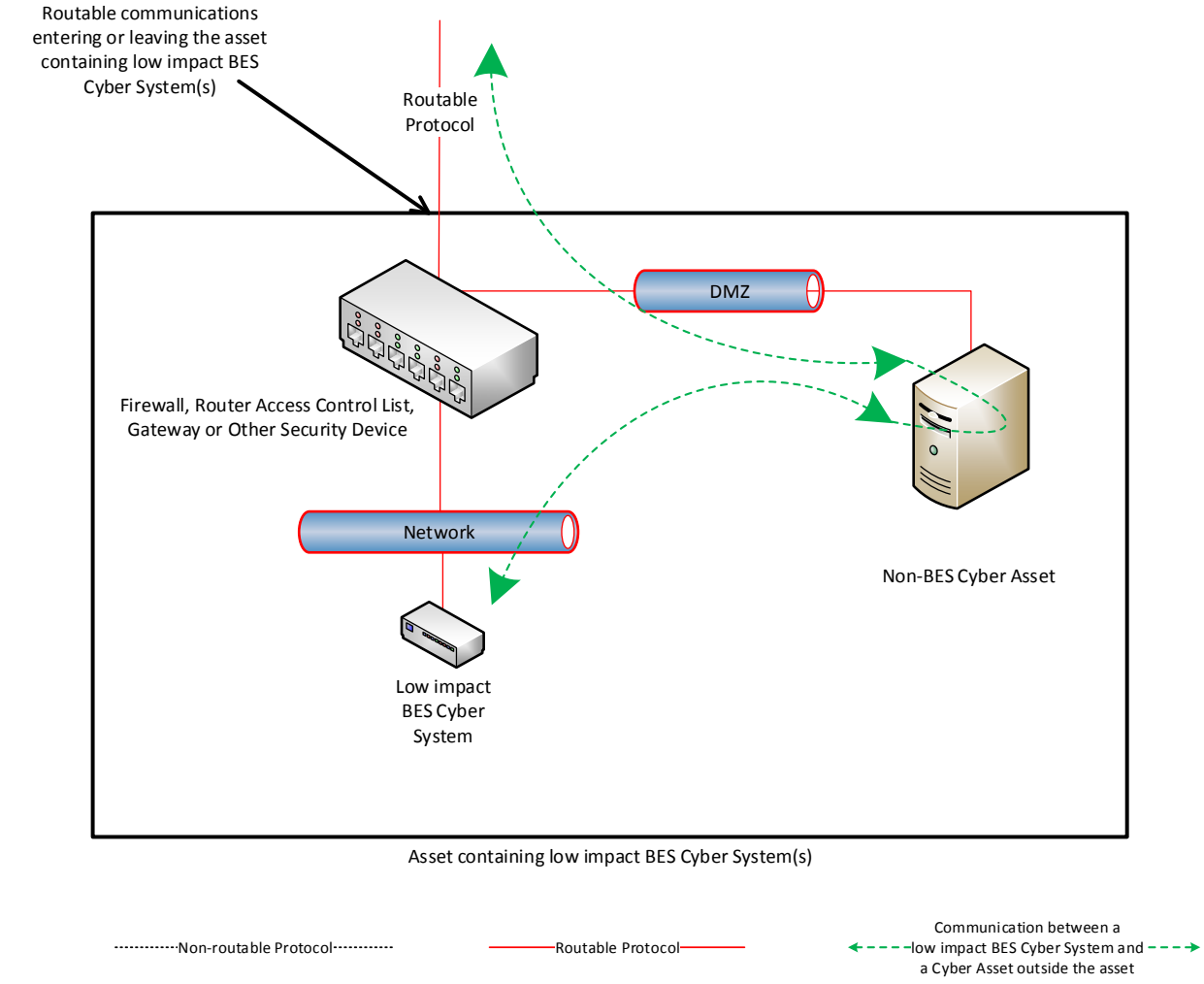
This reference model demonstrates that Responsible Entities have flexibility in choosing their electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication must be configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications may be controlled in this network architecture by permitting no communication be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

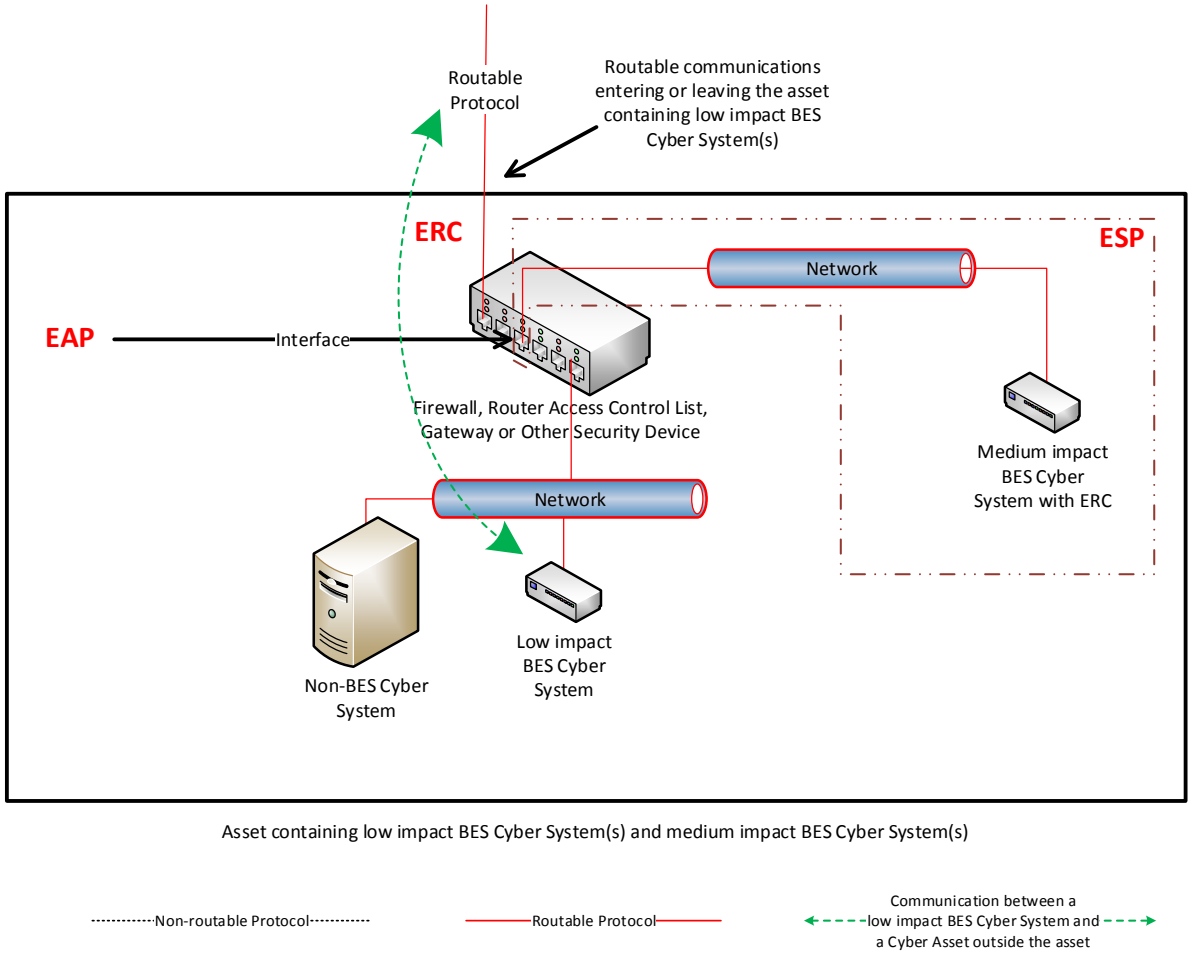
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, the Responsible Entity needs to implement electronic access controls that permit only necessary inbound and outbound electronic access to the BES Cyber System. Consistent with the other reference models provided, this electronic access is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

There is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and ERC present in this reference model because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.



Reference Model 7

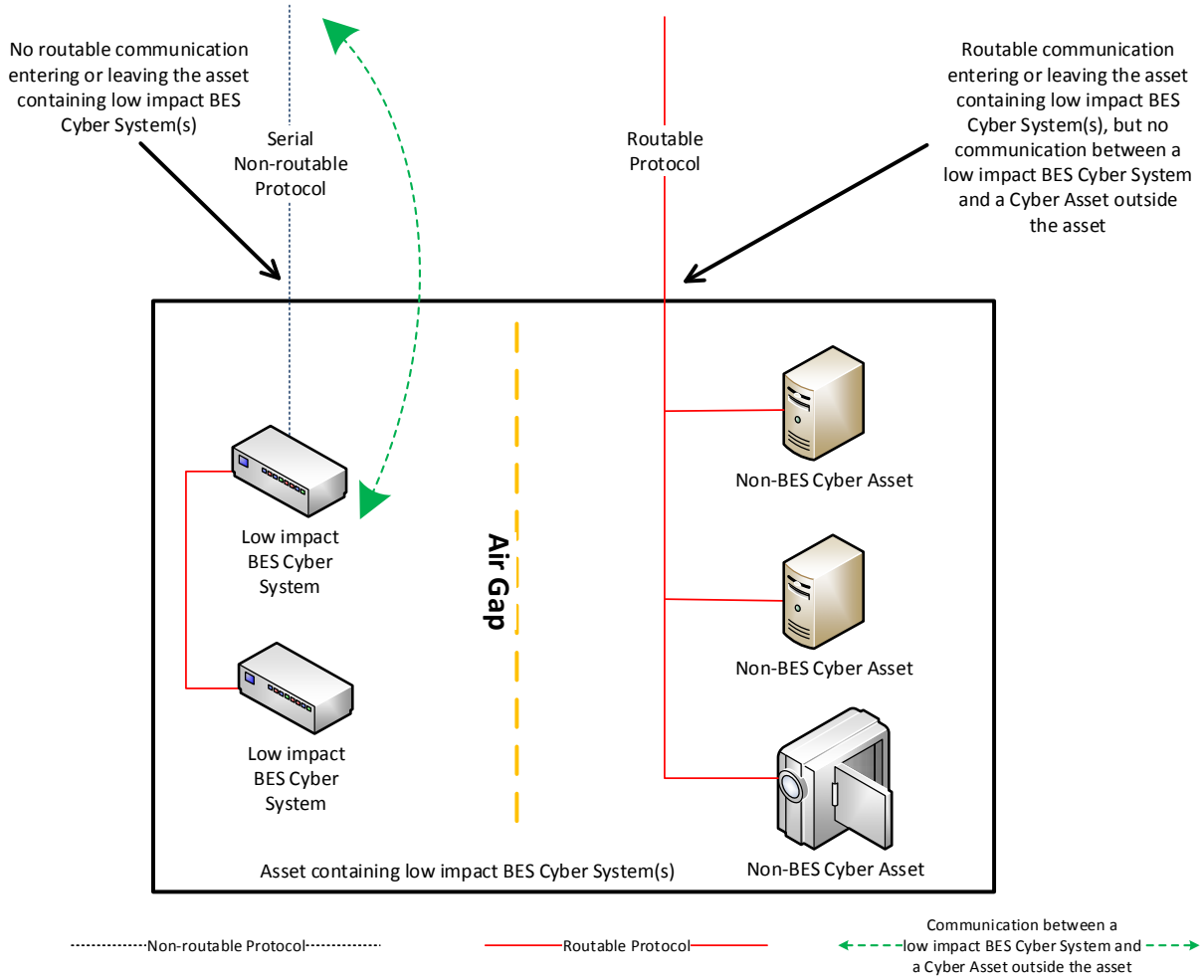
Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria for requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

1) physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;

2) communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls; and

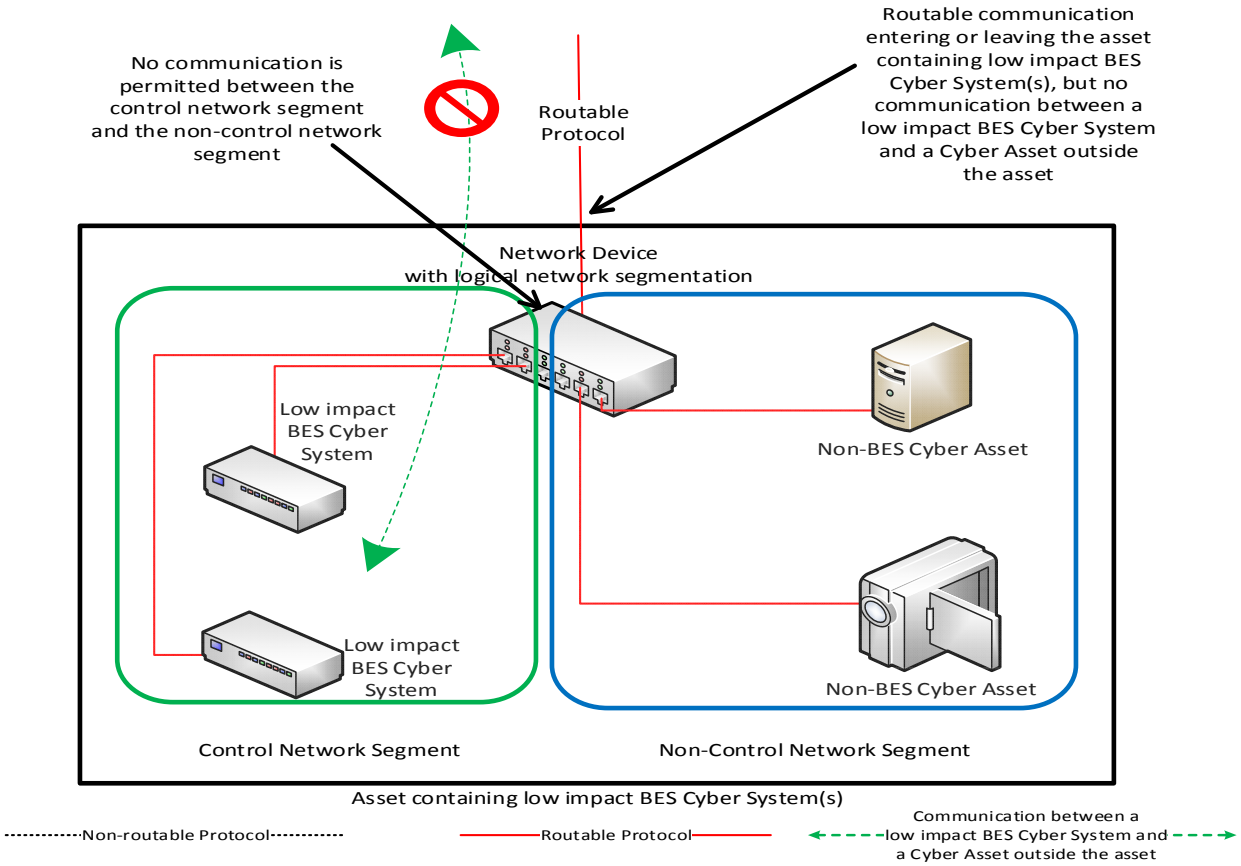
3) routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

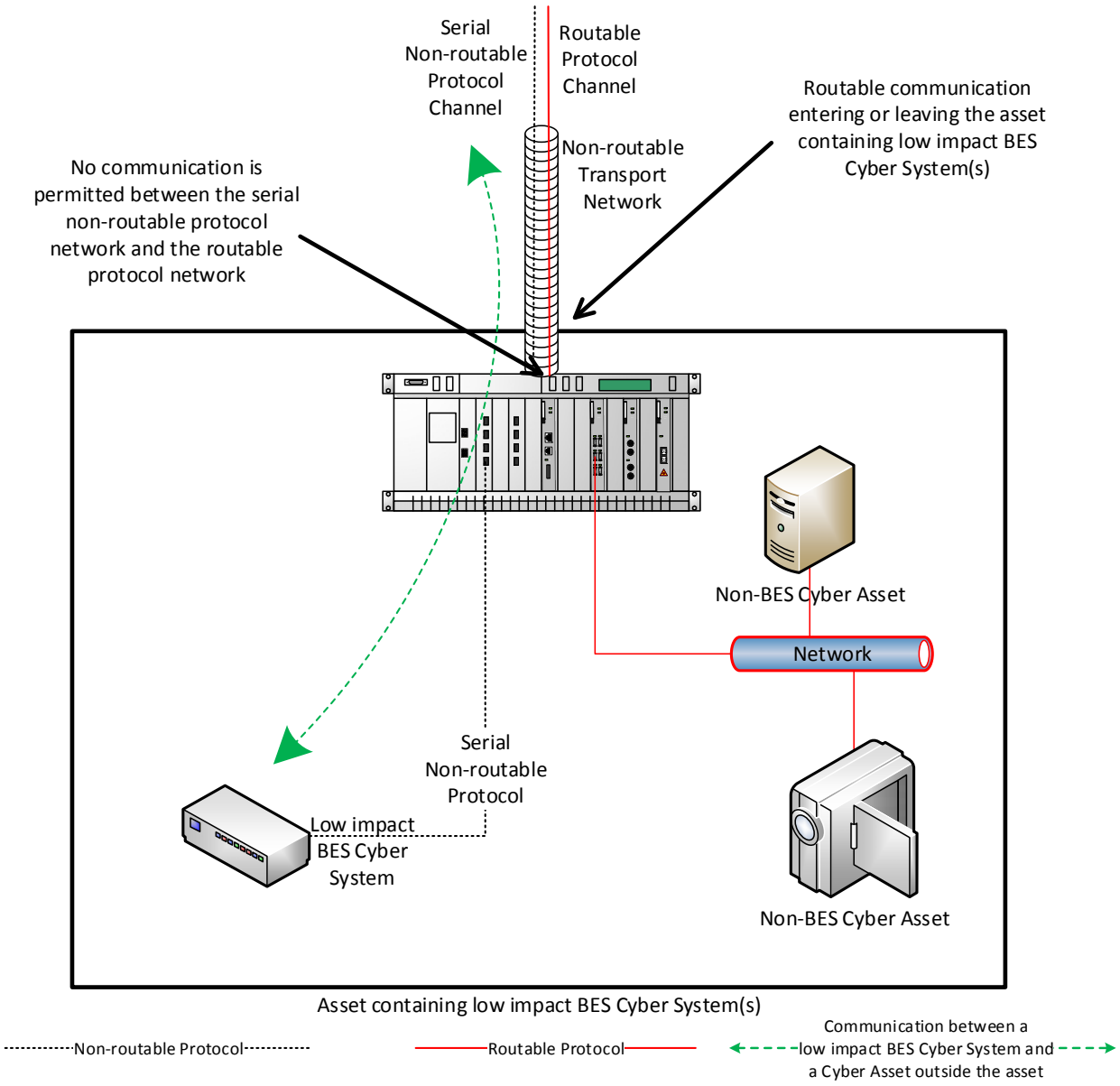
In this reference model, the criteria for requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a non-routable technology, such as a Time-Division Multiplexing (TDM) or Synchronous Optical (SONET) network. In this reference model, the criteria requiring electronic access controls are not met. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol. In similar configurations, the Responsible Entity should closely evaluate the transport entering or leaving the asset containing low impact BES Cyber System(s). If the communication entering or leaving the asset containing low impact BES Cyber System(s) was routable (such as serial encapsulated in TCP/IP or UDP/IP as depicted Reference Model 2 or Reference Model 5), then the criteria requiring electronic access controls would be met.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

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.

Description of Current Draft

This draft of CIP-003-7 is addressing the directive issued by the Federal Energy Regulatory Commission (Commission) in paragraph 73 of Order No. 822 which reads:

> [T]he Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule approving revisions to the cybersecurity Critical Infrastructure Protection (CIP) standards.

~~Previously, the Guidelines and Technical Basis had approximately 10 pages of explanation and numerous reference models to describe different forms of direct vs. indirect access that could be used to determine whether Low Impact External Routable Connectivity existed and thus whether a Low Impact BES Cyber System Electronic Access Point (LEAP) was required.~~

~~In this revision, the term *Low Impact External Routable Connectivity* has been changed to *Low Impact External Routable Communication (LERC)* and simplified so that it is an attribute of a BES asset concerning whether there is routable protocol communications across the asset boundary without regard to 'direct vs. indirect' access that may occur. This greatly simplifies and clarifies the definition of LERC. It removes the dependency between the electronic access controls that may be in place and having those controls determine whether LERC exists or not. For those BES assets that have LERC, the SDT changed the requirement from requiring a LEAP to requiring electronic access controls to "permit only necessary electronic access to low impact BES Cyber Systems" (revised Attachment 1, Section 3.1) within the BES asset and expanded the Guidelines and Technical Basis with numerous examples of electronic access controls.~~

~~Given the modified definition of LERC and~~In this revision, the SDT revised Sections 2 and 3 of Attachments 1 and 2 in CIP-003-7 and removed the terms *Low Impact External Routable Connectivity* (LERC) and *Low Impact BES Cyber System Electronic Access Point* (LEAP). The modifications incorporate concepts and select language from the LERC definition into Attachment 1, Section 3 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). The SDT simplified Section 3 of Attachment 1 to require the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to

implement electronic access controls unless that communication meets the exclusion language (previously in the definition of LERC) contained in (iii) which reads: “not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)”.

The defined term LEAP is no longer necessary because the SDT changed the requirement from requiring a LEAP to requiring electronic access controls. Additionally, since the SDT is removing the term LERC, the exclusion language that was previously in the definition of LERC was integrated into the Attachment 1, Section 3.1 requirement.

Because the proposed modifications ~~in~~to Reliability CIP-003-7~~, there is no longer a~~ eliminate the need for the NERC Glossary ~~term~~terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP~~). Consequently,~~), NERC is ~~proposing that term for retirement.~~

~~In summary, the CIP Standard Drafting Team revised CIP-003-7, Attachments 1 and 2, Sections 2 and 3 and~~ requesting these terms be retired in the associated Implementation Plan.

Additionally, the SDT:

- revised the associated Lower and High VSLs for Requirement R2 to complement the requirement revisions;
- corrected a mistake in the Severe VSL for Requirement R2~~. Non~~;
- made non-substantive changes to the Moderate and High VSLs for Requirement R2 to align with the order of the requirement;
- removed repetitive text from Requirement R1, Part 1.2.3 to make it consistent with Parts 1.2.1 and 1.2.2;
- updated the Guidelines and Technical Basis section of the standard to reflect the revisions made to the Attachments; and
- made non-substantive errata changes ~~were also made within~~throughout the standard~~, including changing~~ such as replacing "ES-ISAC" ~~to~~with "E-ISAC".

Completed Actions	Date
Standard Authorization Request (SAR) approved	July 20, 2016
Draft 1 of CIP-003-7 posted for formal comment and initial ballot	July 21 – September 6, 2016
Draft 2 of CIP-003-7 posted for formal comment and additional ballot	October 21 – December 5, 2016

Anticipated Actions	Date
10-day final ballot	~~October, 2016~~January, 2017
NERC Board of Trustees (BOT) adoption	~~November, 2016~~February, 2017
Petition filed with FERC	March, 2017

A. Introduction

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

2. **Number:** CIP-003-7

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 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 SPS or RAS where the SPS or 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-003-7:

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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3 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.

4.2.3.4 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-003-7.

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single

cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls ~~for Low Impact External Routable Communication (LERC) and Dial-up Connectivity~~; and

1.2.4. Cyber Security Incident response

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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None~~.~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but	The Responsible Entity failed to document ~~or~~and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2~~).~~)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans	containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented	failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2)	its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification,	The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) ~~OR~~ ~~The Responsible Entity documented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to implement the electronic access controls according to Requirement R2,~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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	~~Attachment 1, Section 3. (R2)~~ ~~OR~~ ~~The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(E-ISAC) according to Requirement R2, Attachment 1, Section 4. ~~(R2)~~ ~~OR~~ ~~The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)~~ ~~OR~~ ~~The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed~~		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)~~		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name,	The Responsible Entity has identified a delegate by name,	The Responsible Entity has identified a delegate by name, title, date of	The Responsible Entity has used delegated authority

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			title, date of delegation, and specific actions delegated, but 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. (R4)	title, date of delegation, and specific actions delegated, but 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. (R4)	delegation, and specific actions delegated, but 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. (R4)	for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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.	

Version	Date	Action	Change Tracking
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 devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees.	Revised to address FERC Order 822 directive regarding definition of LERC.

Attachment 1

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

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

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

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

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security control objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition…within one year of the effective date of this Final Rule.

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the exclusion language (previously in the definition of LERC) contained in (iii) which reads: "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The

focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

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

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

3.1 ~~Implement~~Permit only necessary inbound and outbound electronic access ~~control(s)~~ as determined by the Responsible Entity for ~~LERC, if~~ any~~, to permit only necessary electronic access to~~ communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. ~~Implement authentication for~~using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and,

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Attachment 2

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

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

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

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

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

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

1. Documentation, such as representative diagrams or lists of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; ~~authenticating users; air gapping networks; terminating routable protocol sessions on a non-BES Cyber Asset;~~ implementing unidirectional gateways) showing that ~~for LERC~~ at each asset or group of assets containing low impact BES Cyber Systems, ~~is confined~~routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only ~~to~~ inbound and outbound electronic access that ~~access~~ the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices; and
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must

be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems~~, also referred to herein as BES assets~~, the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in

NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts

- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

~~Using the list of assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement~~The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that ~~addresses~~address the security objective ~~criteria~~ for the protection of low impact BES Cyber Systems. ~~The protections required by Requirement R2 reflect the level of risk that misuse or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the~~The required protections are designed to

be part of a program that covers the low impact BES Cyber Systems collectively ~~either~~ at an asset ~~or site~~ level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

~~There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and Dial-up Connectivity, and (4) Cyber Security Incident response.~~

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. ~~Guidance for each of the four subject matter areas of Attachment 1 is provided below~~The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The Responsible Entity is not required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the ~~BES~~same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls outlined in Section 2, this can be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility ~~in the selection of~~to select the methods used to meet the objective ~~to control~~of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves~~, as well as physical protection of~~ and (2) the electronic access control Cyber Assets specified by the Responsible

Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. ~~User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.~~

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level ~~for access to the site or systems.~~. The requirement does not obligate an entity to specify a need for each physical access or authorization of ~~a user~~an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems~~, also referred to herein as BES assets~~ when ~~external~~there is routable protocol communication ~~(LERC)~~ or Dial-up Connectivity ~~is present to or from~~between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s~~),~~) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. ~~In the case where there is no LERC or Dial-up Connectivity, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s).~~

When implementing Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low

impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, Responsible Entities are to determine ~~LERC~~whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity ~~for their BES assets and then, if~~ to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s).

~~Determining LERC~~

~~The defined term Low Impact External Routable Communication (LERC) is used to avoid confusion with the term External Routable Connectivity (ERC) used for high and medium impact BES Cyber Systems as these terms~~ Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are ~~different concepts.~~ not required to establish any specific electronic access controls.

The ~~input~~inputs to this requirement ~~from~~ are the assets identified in CIP-002 ~~is a list of assets~~as containing low impact BES Cyber ~~Systems,~~System(s); therefore ~~LERC is an attribute of a BES asset and involves~~, the determination of routable protocol communications ~~to or from the BES asset (crossing the asset boundary) without regard to connectivity to Cyber Assets within the BES asset. ERC on the other hand~~ or Dial-up Connectivity is an attribute of ~~an individual high or medium impact BES Cyber System and is relative to an Electronic Security Perimeter (ESP).~~

~~With LERC being a BES asset level attribute, it is used as a higher level filter to exclude from further consideration those assets containing low impact BES Cyber Systems that have no routable protocol communications to them from outside the BES asset. Responsible Entities can then concentrate their electronic access control efforts on those BES assets that do have LERC.~~the asset. However, ~~this also means that LERC can exist for a BES asset even if there is no routable protocol connectivity to any~~ any communication that provides no access to or from the low impact BES Cyber System ~~within the BES asset~~(s), but happens to be located at the asset with the low impact BES Cyber System(s), does not require evaluation for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the ~~LERC definition specifically excludes~~obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions ~~between non-Control Center BES assets containing low impact BES Cyber Systems~~, such as IEC TR-61850-90-5 R-GOOSE messaging. ~~This does not exclude Control Center to field communication but rather excludes the communication between the intelligent electronic devices (e.g. relays) in the field~~Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While

technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive ~~requirements~~characteristics related to this technology ~~nor~~and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining ~~Asset Boundary~~Routable Protocol Communications

~~As LERC is a BES asset level attribute, it involves a determination by the~~ In order for Responsible ~~Entity of~~Entities to determine whether electronic access controls need to be implemented, the Responsible Entity needs to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that use a ~~BES~~ routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach to making this evaluation. One approach is for Responsible Entities to identify an "electronic boundary~~ for their assets containing low impact BES Cyber Systems. This~~" associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary ~~will~~may vary by ~~BES~~ asset type (Control Center, substation, generation resource) and the specific configuration of the ~~BES~~ asset. ~~The~~If this approach is used, the intent is for the Responsible Entity to define the ~~BES asset~~electronic boundary such that the low impact BES Cyber System(s) ~~that are~~ located at the ~~BES~~ asset are contained within the ~~BES asset~~"electronic boundary~~.~~." This is strictly for determining ~~what constitutes the BES "asset" and for determining~~ which routable protocol communications and networks are internal or inside or local to the ~~BES~~ asset and which are external to or outside the ~~BES asset. This is not an Electronic Security Perimeter or Physical Security Perimeter as defined for medium and high impact BES Cyber Systems. For the asset containing low impact BES Cyber System(s), the BES asset boundary is synonymous to the concept of a "logical border" demarcation where routable protocol communication (e.g. LERC) enters and exits the BES asset containing the low impact BES Cyber System. Some examples of ways a~~ asset.

Alternatively, the Responsible Entity may ~~determine BES~~find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset ~~boundaries are:~~demarcation to ensure that the electronic access controls

are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

- For Control Centers
  - Designated areas (room(s) or floor(s)) if the Control Center is located within a larger building.
  - A building if in a dedicated building on a shared campus.
  - The property/fence line if the Control Center is a dedicated facility on dedicated property.
- For substations, this could be the property/fence line or the control house.

- For generation resources:
  - Fossil/hydro generating facilities: This could be the property/fence line. If pumps or wells or other equipment that are part of the plant asset are outside the property line, then the BES asset boundary could expand to accommodate all that is considered part of the plant.
  - Solar farms: This could be the property line(s) or fence(s) surrounding all solar panels and interconnection facilities.
  - Wind farms: This could be the collection of individual turbines plus the equipment needed for interconnection.
  - Cogeneration facilities: This could be the identified portion of the larger plant that performs generation.

Determining Electronic Access Controls

Once a Responsible Entity has determined that LERC exists atthere is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the BES asset boundary,containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the Responsible Entity documents and implements its chosen electronic access control(s). The control(s) must allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity and they need to. The Responsible Entity must be able to explain the reasons for the electronic access permitted with their electronic access controls.. The reasoning for the "necessary" inbound and outbound electronic access controls can be documented within the Responsible Entity's cyber security plan(s) or other policies or procedures associated with the electronic access controls.

Concept Diagrams

The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the security objective of permitting only necessary inbound and outbound electronic access tofor communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset must be met when there is LERC to a BES asset.

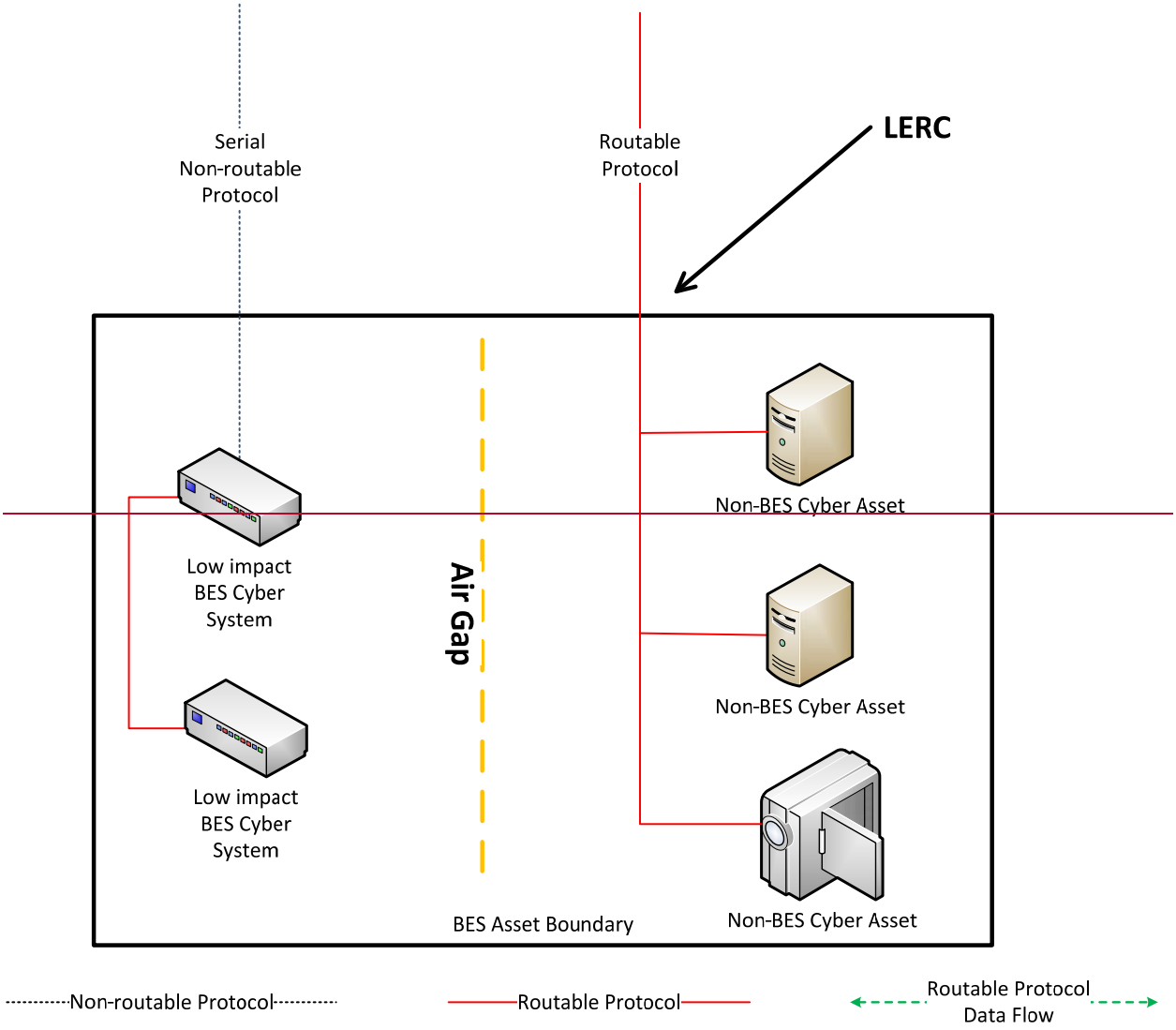
NOTE:

- This is not an exhaustive list of applicable concepts.
- LERC is present in each diagram.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.
- The term "BES Asset Boundary" is capitalized in the diagrams but it is not a defined term.

~~LERC~~

Reference Model 1~~— Physical Isolation~~

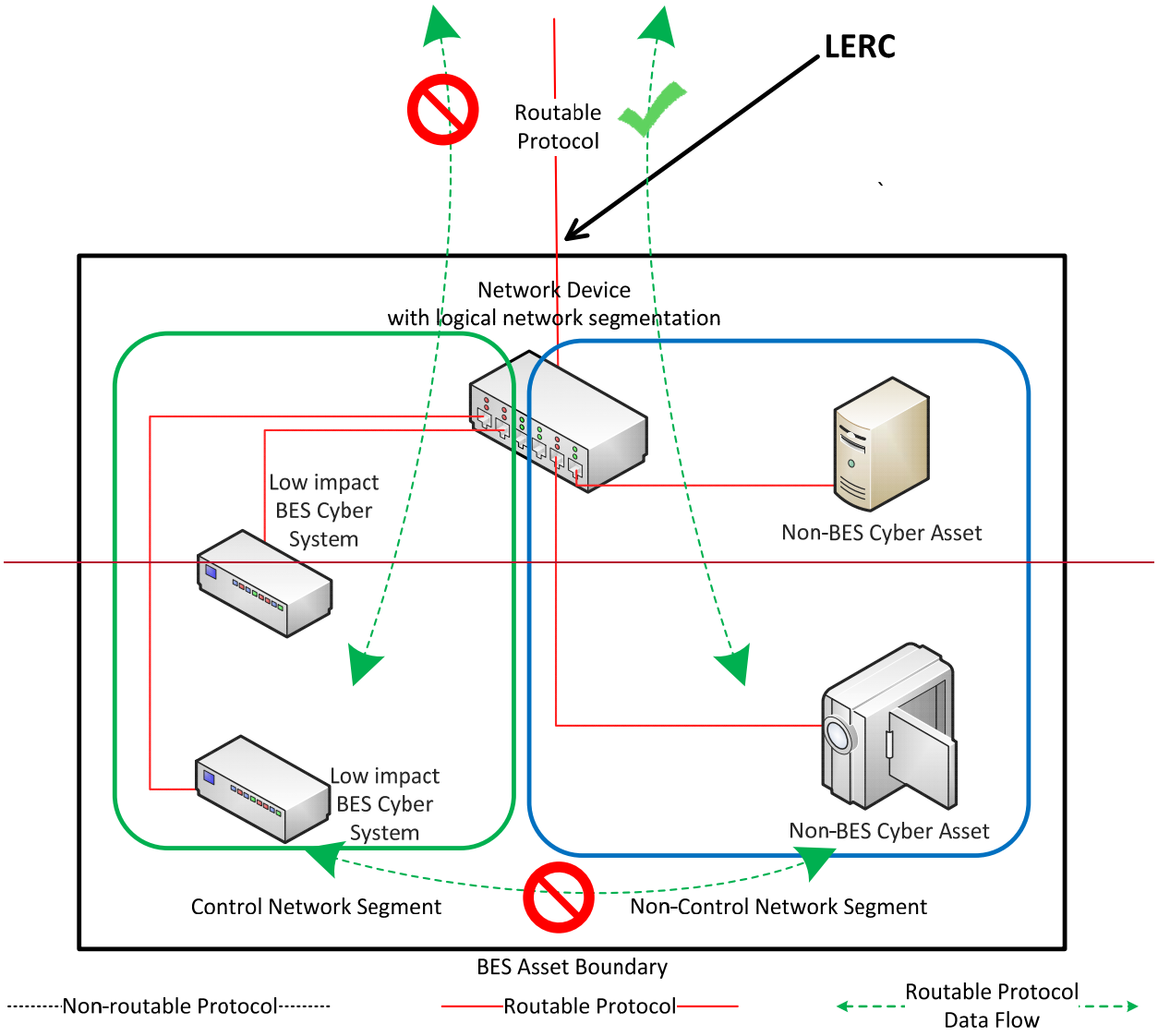
~~The Responsible Entity may choose to physically isolate the low impact BES Cyber System(s) from the LERC. This control is commonly referred to as an 'air gap'. The serial non-routable protocol connection and the routable protocol LERC are completely isolated from each other. There is no equipment shared with the low impact BES Cyber System(s).~~



~~*Reference Model 1*~~

~~**LERC Reference Model 2 – Logical Isolation**~~

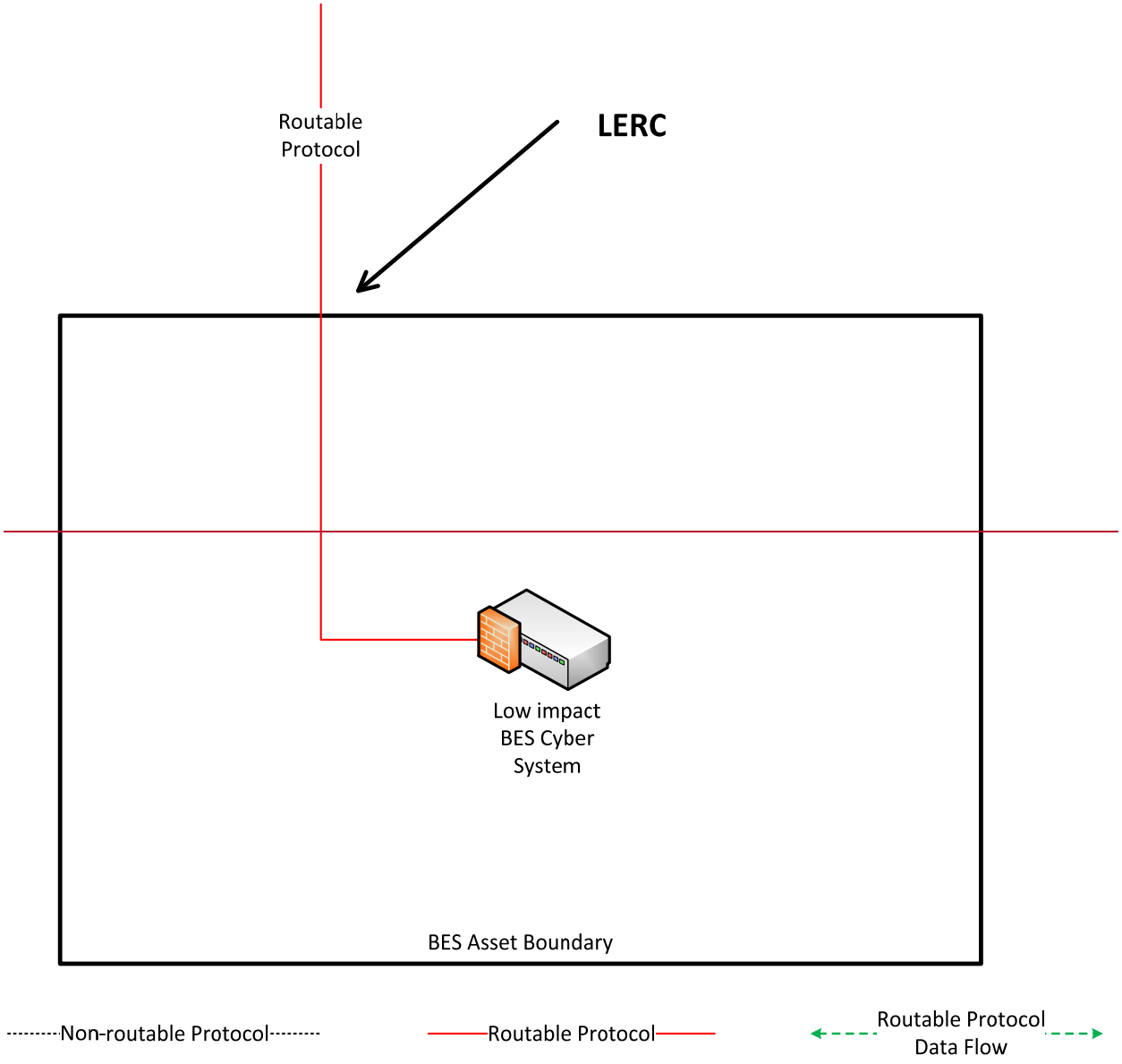
~~The Responsible Entity may choose to logically isolate the low impact BES Cyber System(s) from the LERC. The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s).~~

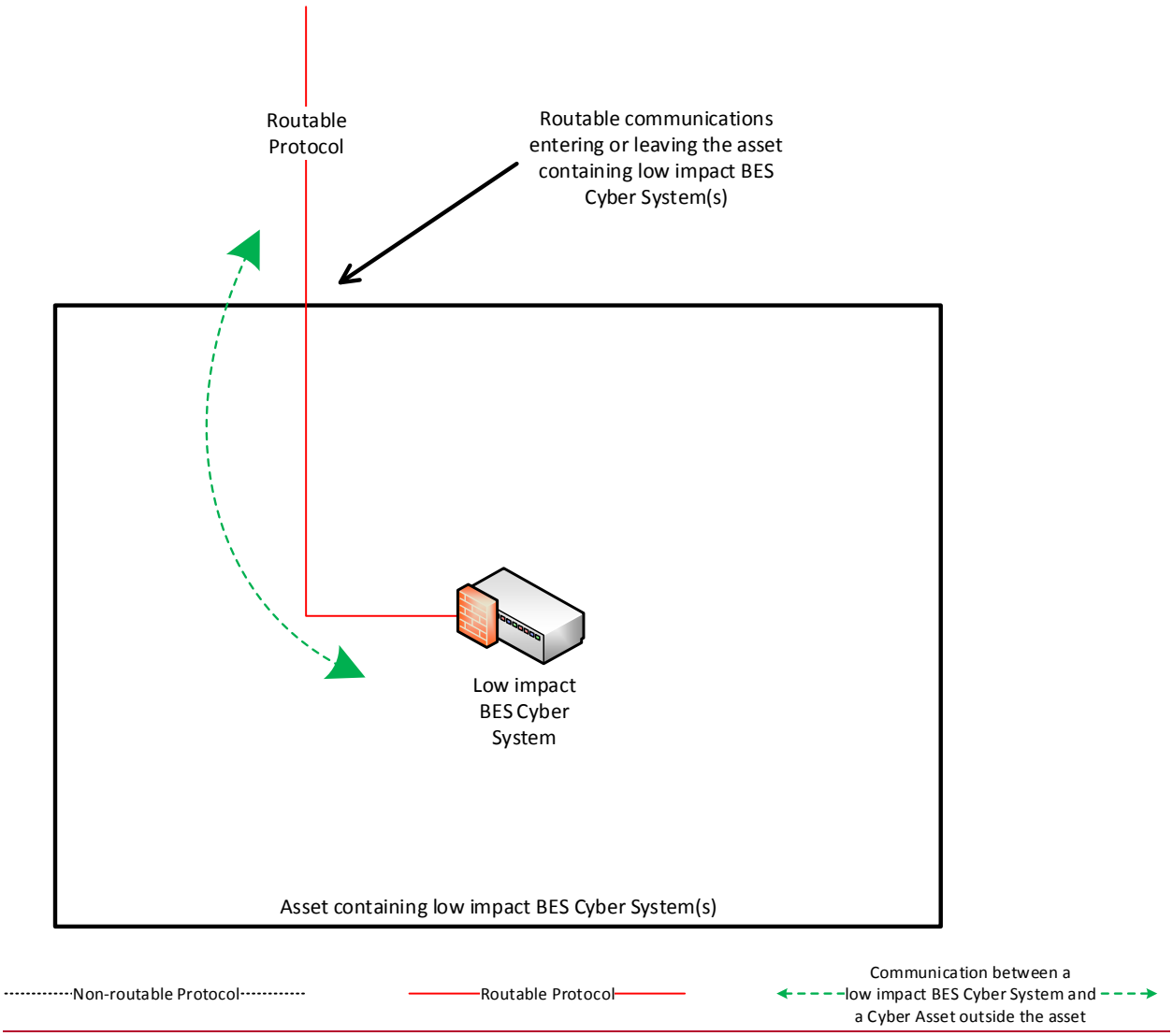


~~*Reference Model 2*~~

~~LERC Reference Model 3~~ – Host-based Inbound & Outbound Access Permissions

The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access ~~permission~~permissions so that only necessary inbound and outbound routable protocol access is allowed ~~to the low impact BES Cyber System(s).~~between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary. Responsible Entities may further restrict electronic access using ports and services based on the capability of the electronic access control, low impact BES Cyber System, application, etc.

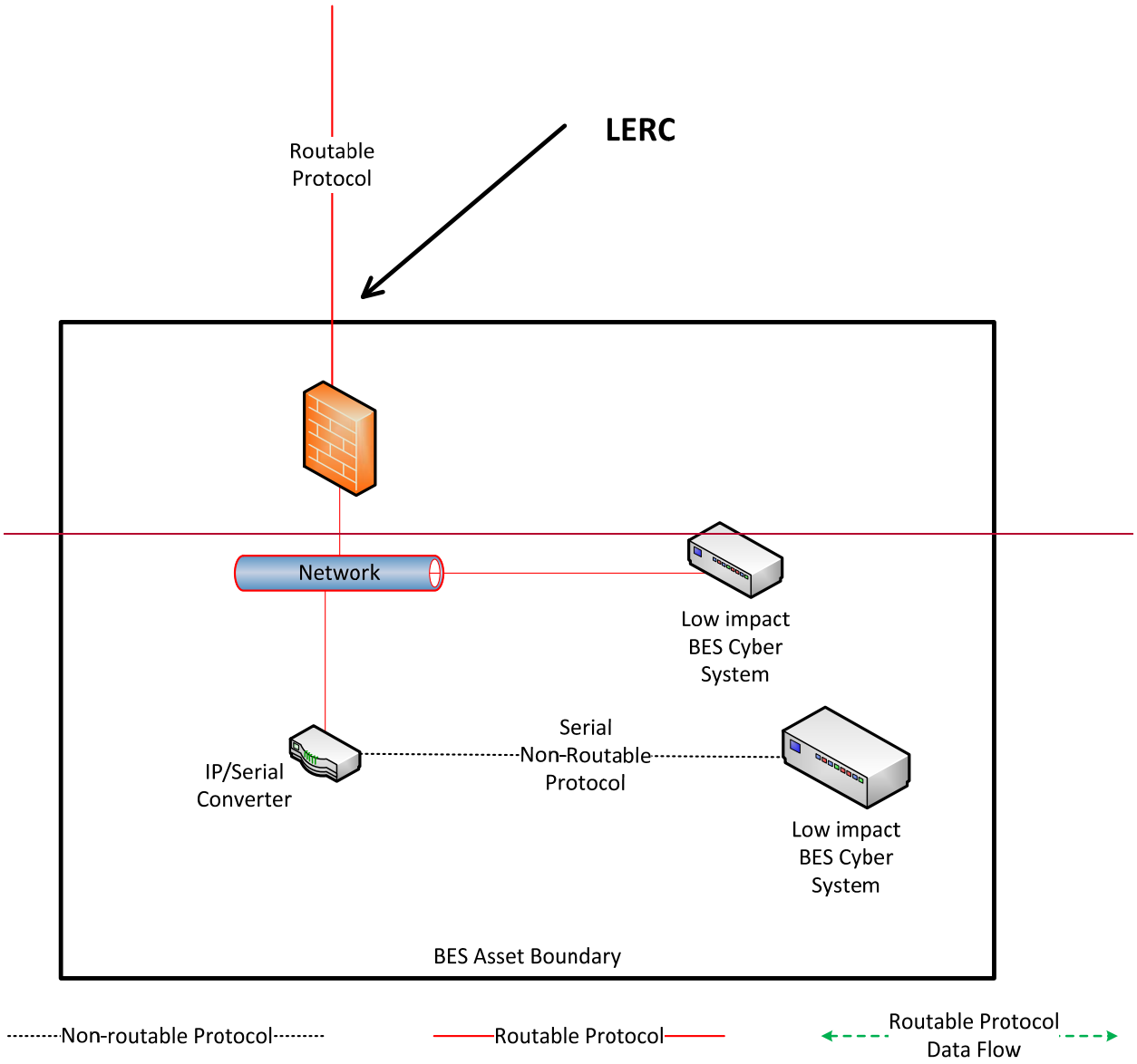

Routable
Protocol
LERC
Low impact
BES Cyber
System
BES Asset Boundary
Non-routable Protocol
Routable Protocol
Routable Protocol
Data Flow

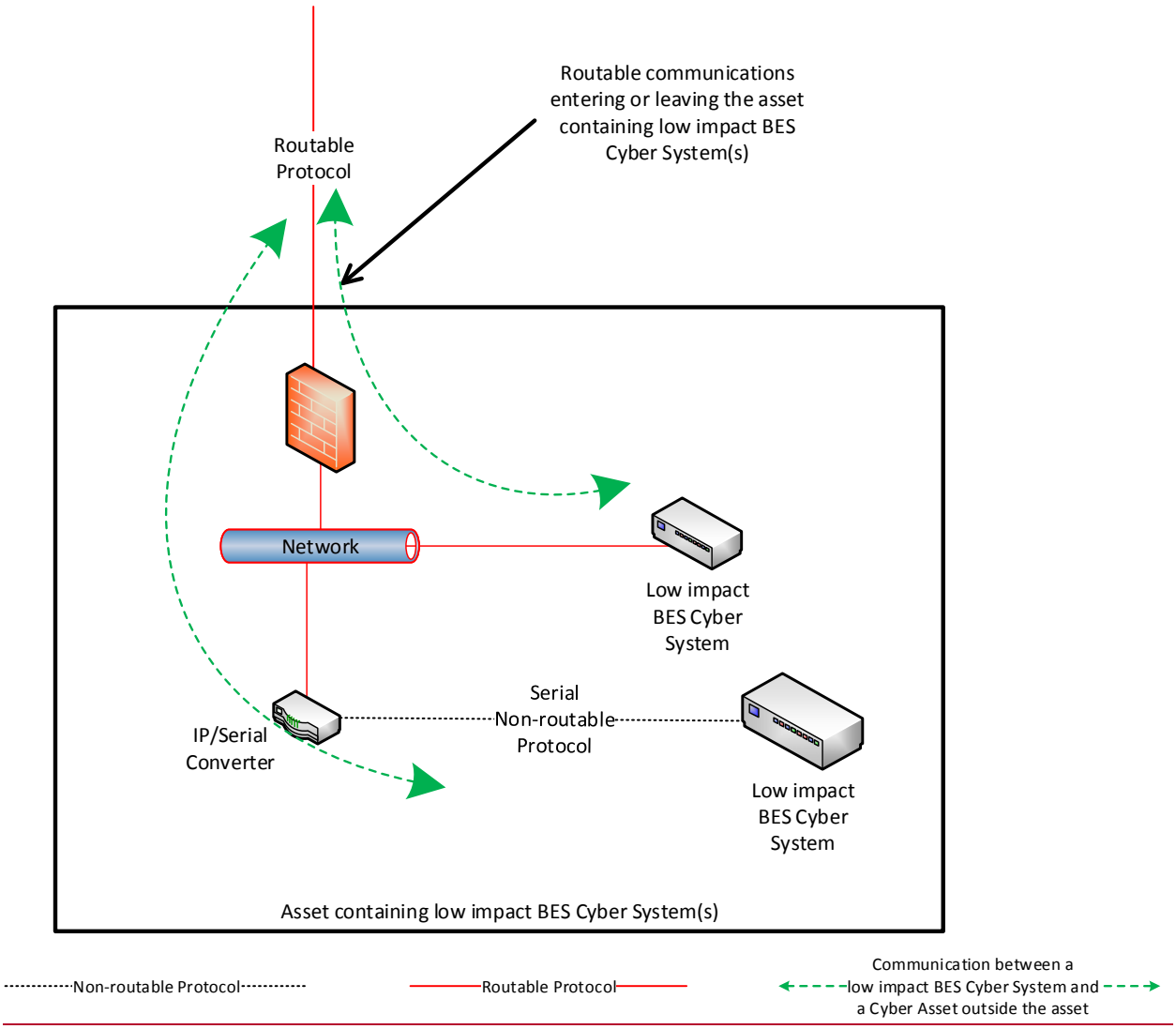


Reference Model ~~3~~1

~~LERC~~ Reference Model ~~4~~2 – Network-based Inbound & Outbound Access Permissions

The Responsible Entity may choose to ~~utilize~~use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the ~~BES asset.~~asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed ~~over the LERC as the~~using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from ~~device~~the Cyber Asset(s) that are outside the ~~BES~~ asset ~~boundary~~ to the low impact BES Cyber ~~Systems.~~System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber ~~Systems~~System(s). When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary. Responsible Entities may further restrict electronic access using ports and services based on the capability of the electronic access control, low impact BES Cyber System, application, etc.


LERC
Routable Protocol
Network
Low impact BES Cyber System
Serial Non-Routable Protocol
IP/Serial Converter
Low impact BES Cyber System
BES Asset Boundary
Non-routable Protocol
Routable Protocol
Routable Protocol Data Flow

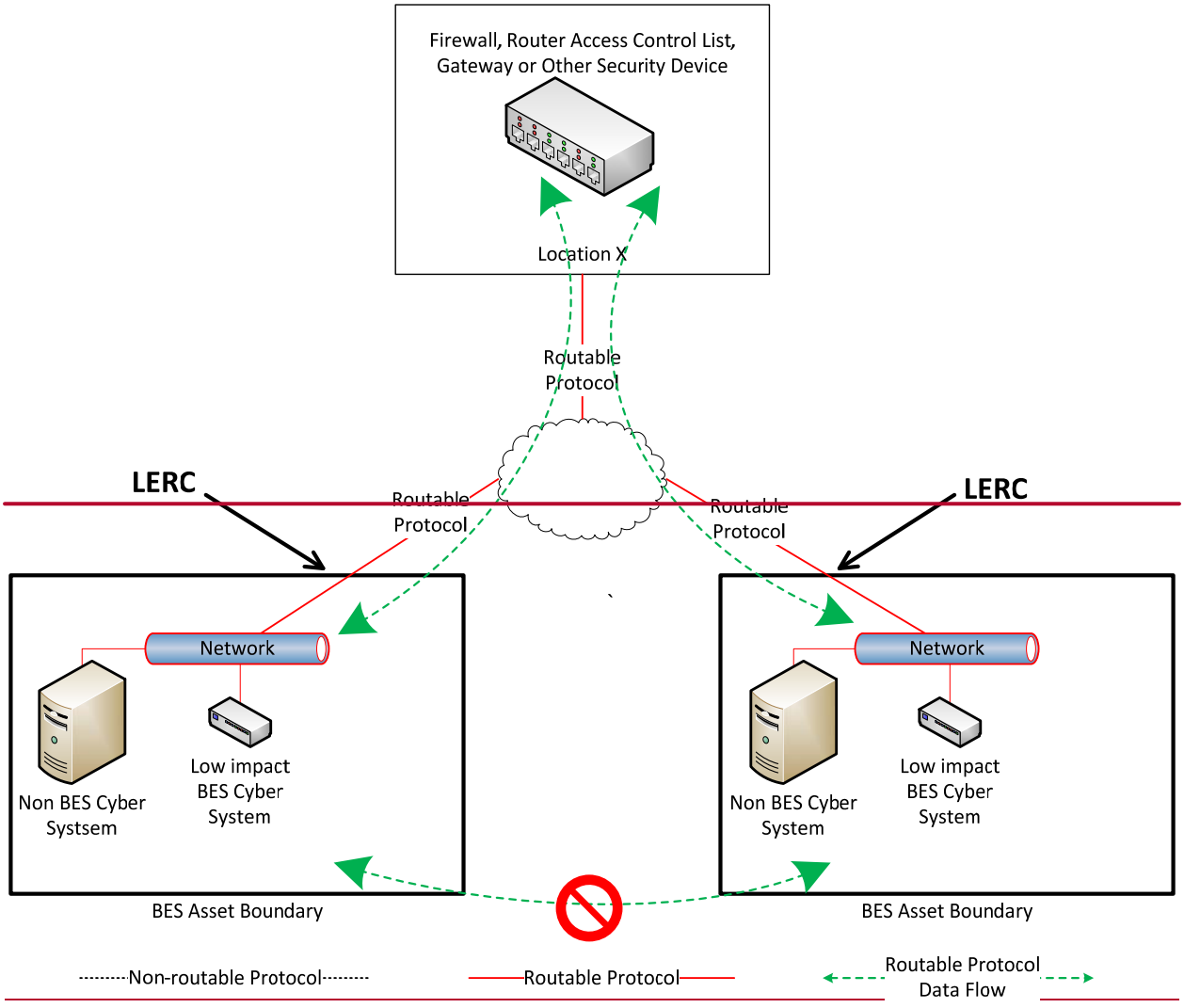


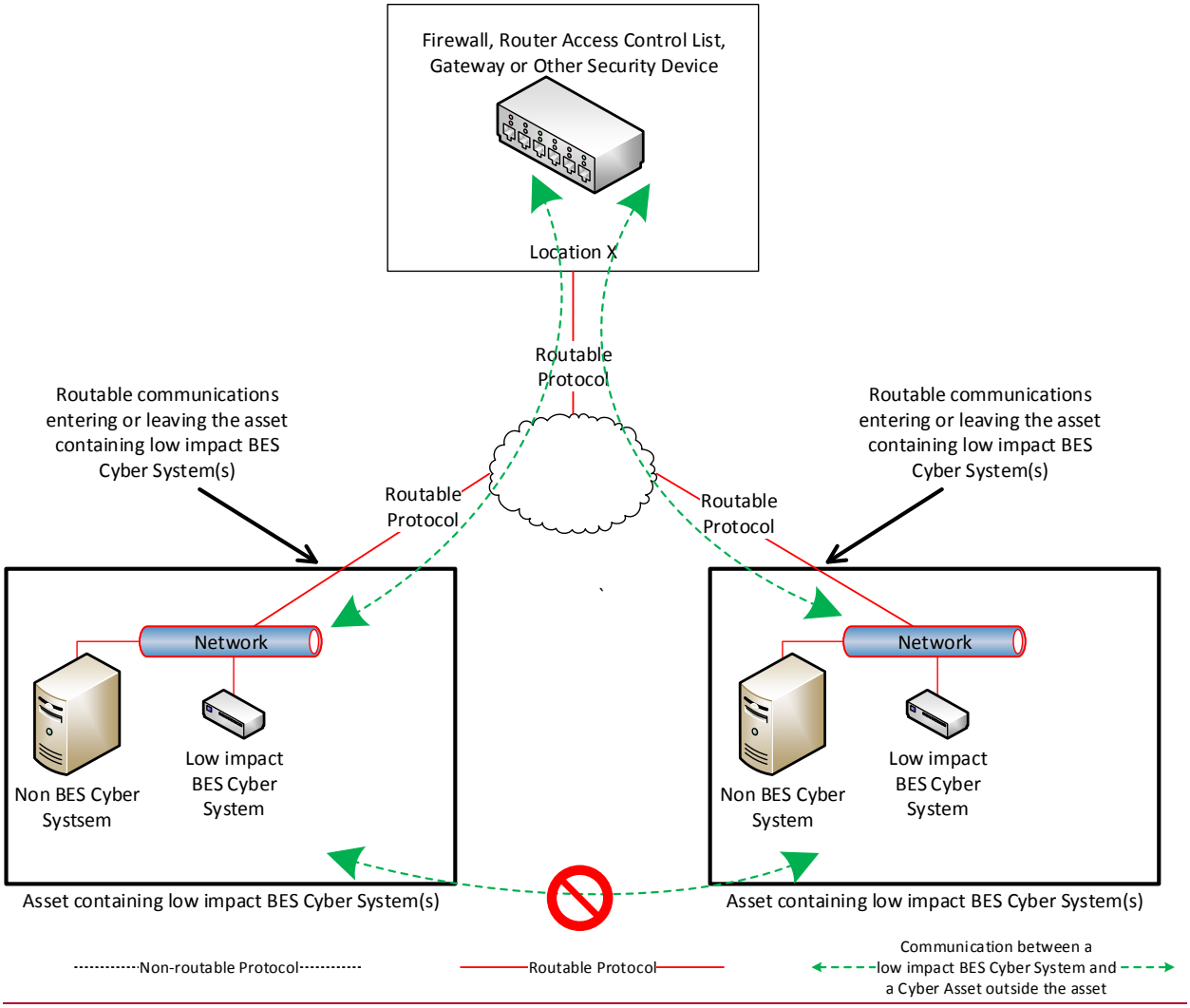
Reference Model 2

Reference Model 4

~~LERC Reference Model 5~~3 – Centralized Network-based Inbound & Outbound Access Permissions

The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be another ~~BES asset.~~asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access ~~to~~between the low impact BES Cyber System(s~~).~~) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each ~~BES~~ asset is through the electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary. Responsible Entities can further restrict electronic access using ports and services based on the capability of the electronic access control, low impact BES Cyber System, application, etc.

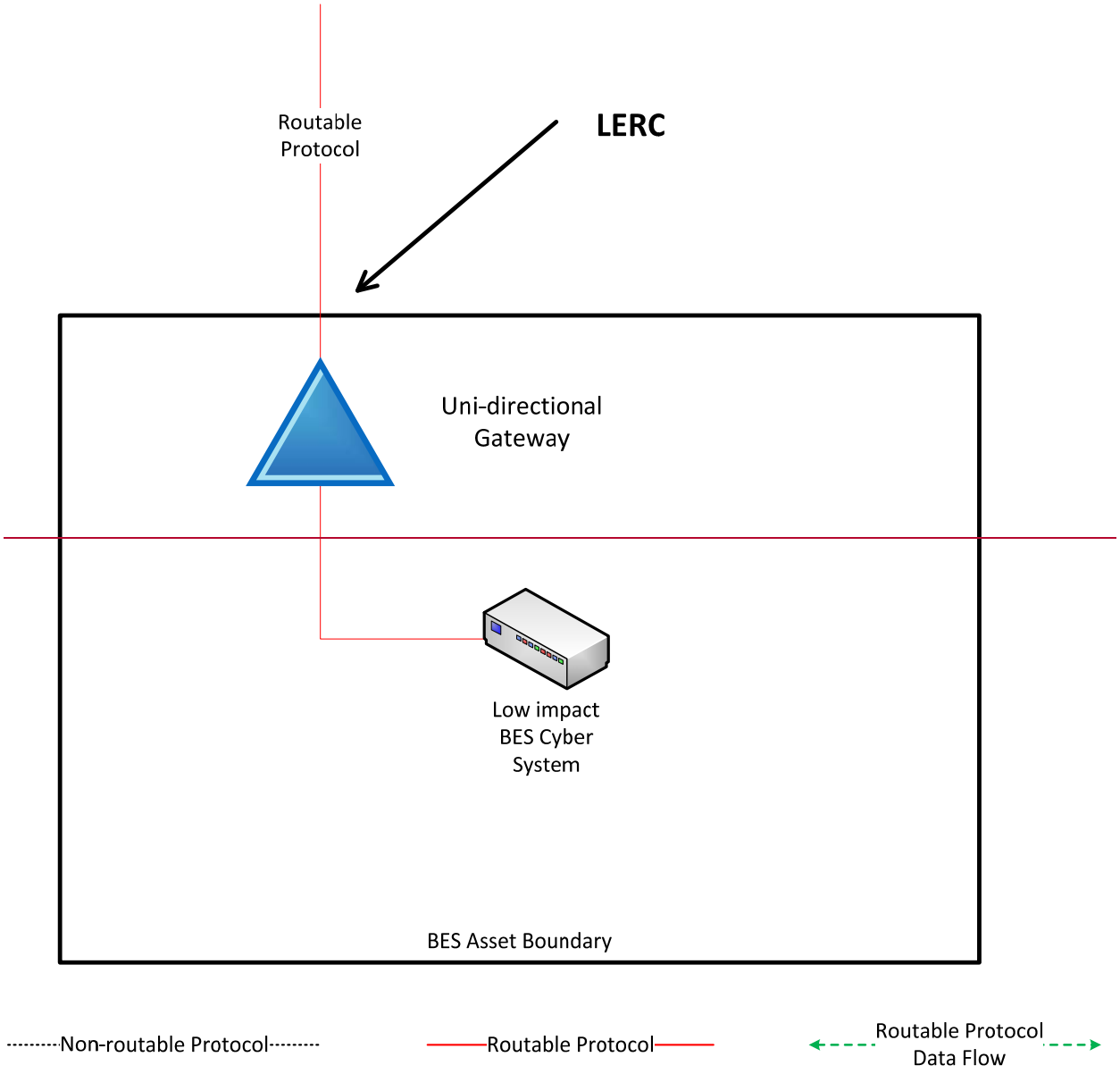


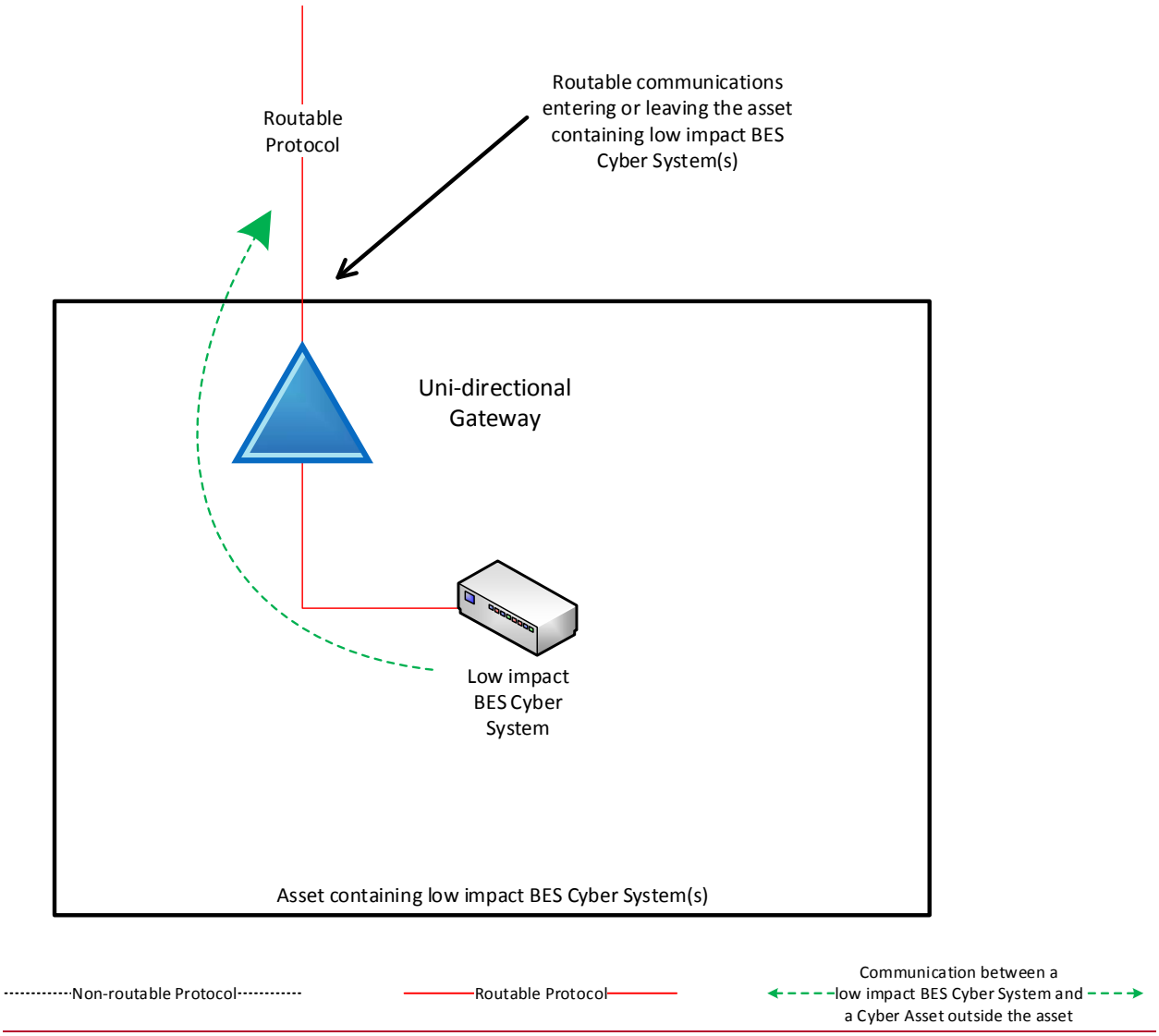


Reference Model ~~5~~3

~~LERC~~ Reference Model ~~6~~4 – Uni-directional Gateway

The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) ~~from~~using the ~~LERC~~routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow ~~across the BES asset boundary~~. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.

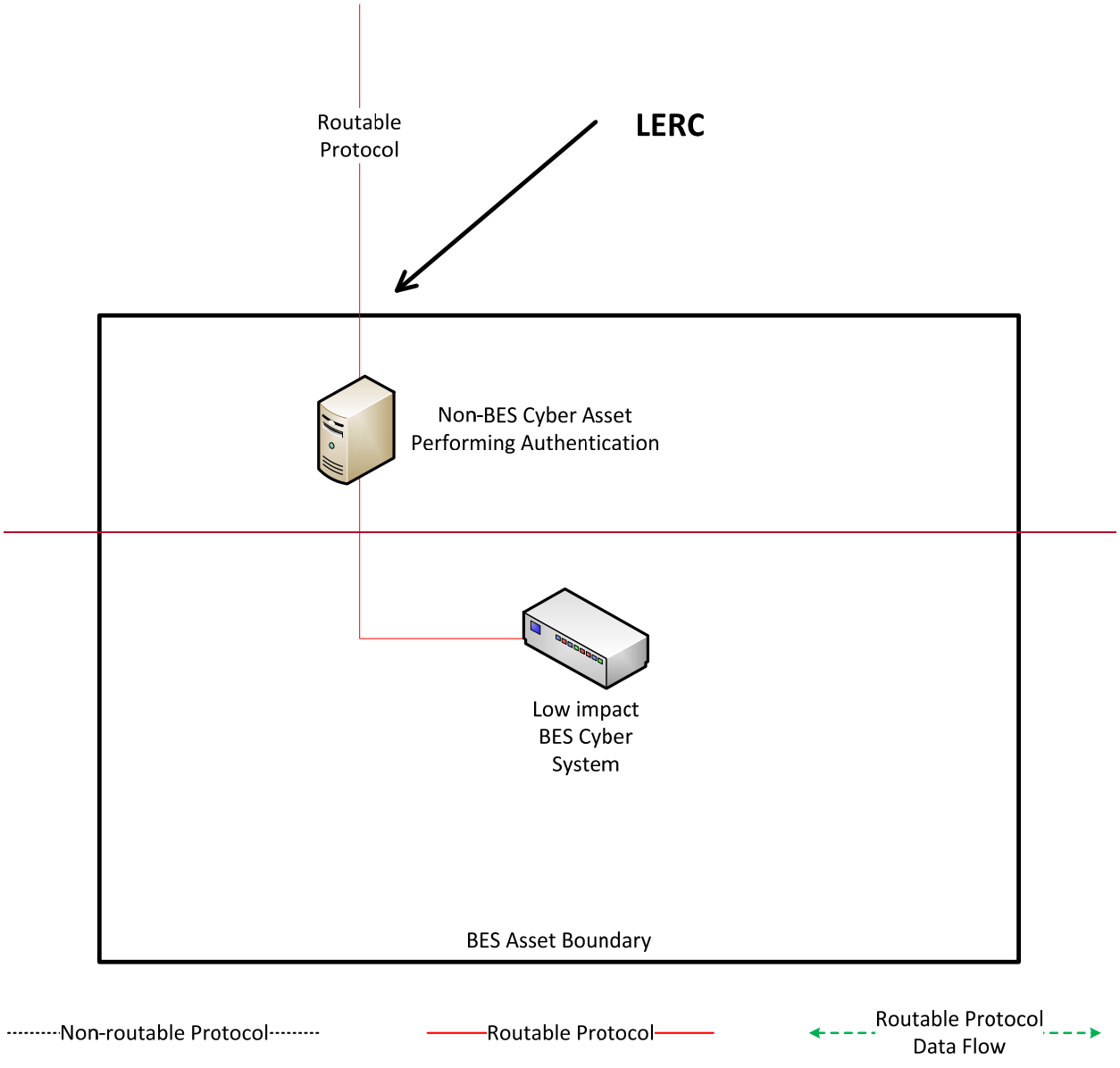

Routable Protocol
LERC
Uni-directional Gateway
Low impact BES Cyber System
BES Asset Boundary
Non-routable Protocol
Routable Protocol
Routable Protocol Data Flow



Reference Model ~~6~~4

~~LERC~~ Reference Model ~~7~~5 – User Authentication

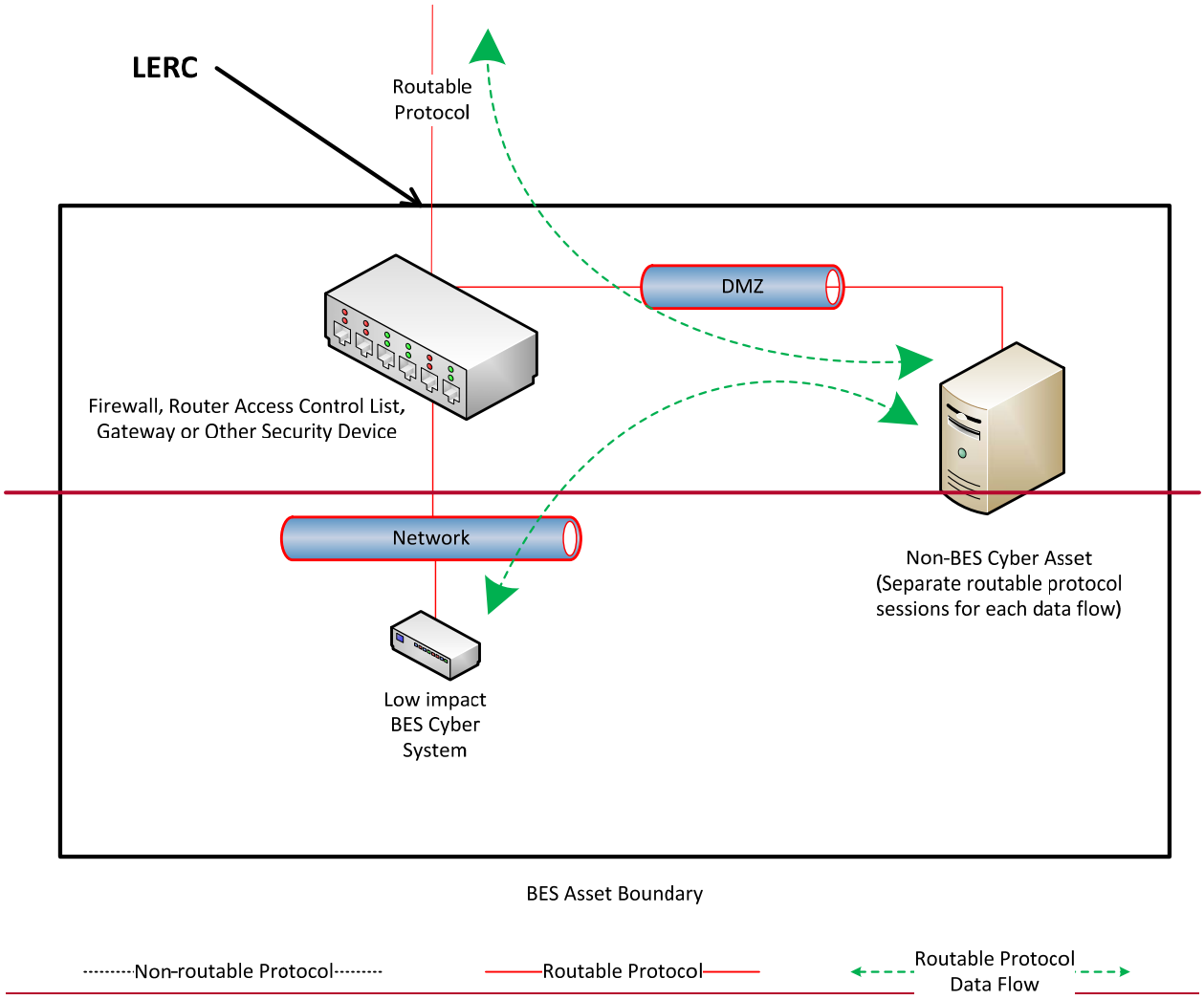
~~The Responsible Entity may choose to utilize a non-BES Cyber Asset between the network outside the BES asset boundary and the low impact BES Cyber System to perform user authentication for interactive access. The non-BES Cyber Asset would require authentication before establishing a new connection to the low impact BES Cyber System. The electronic access control depicted in this reference model may not meet the security objective for controlling device-to-device communication across the LERC depending on the specific system configuration in place.~~



~~*Reference Model 7*~~

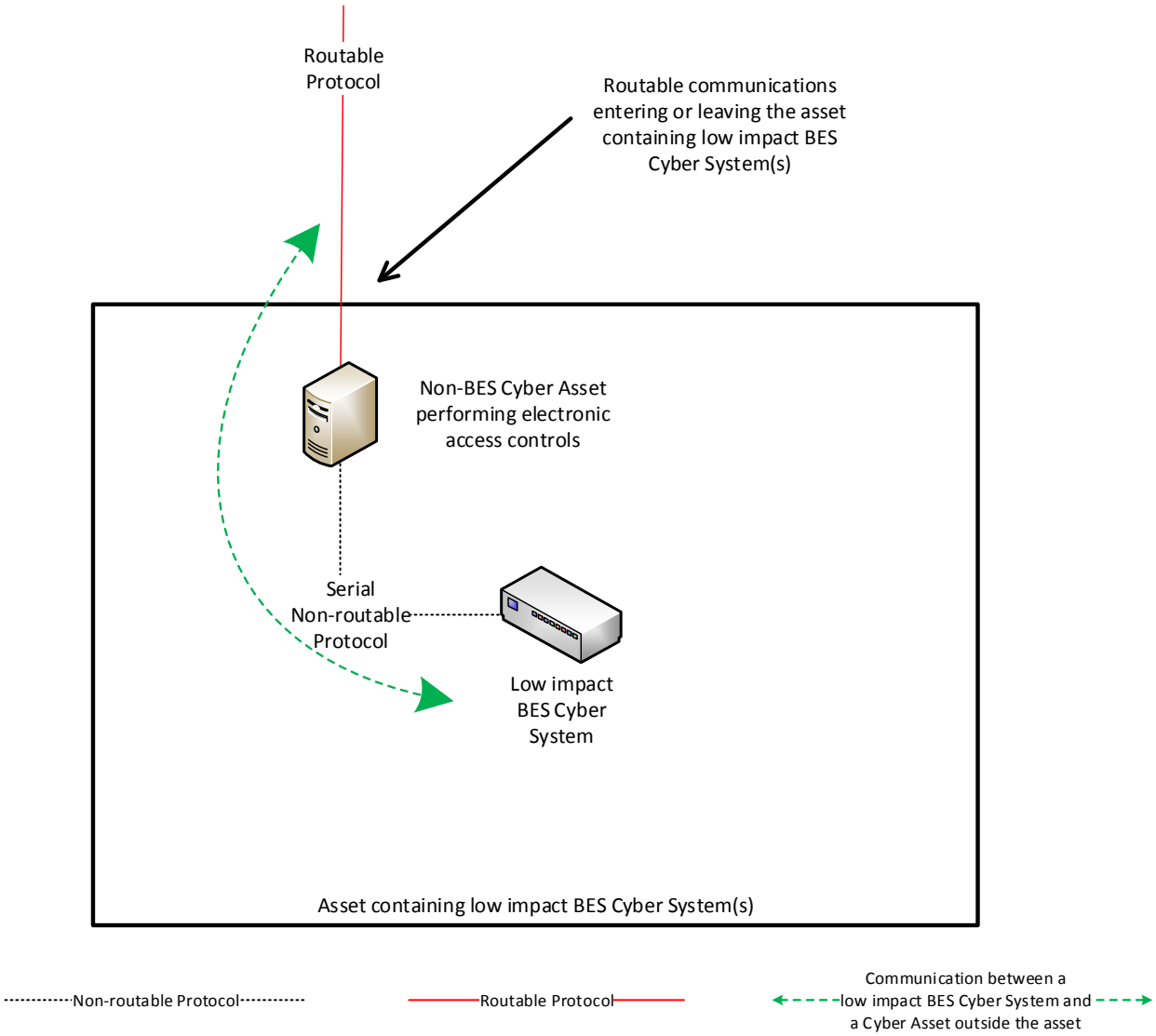
~~**LERC Reference Model 8 – Session Termination**~~

~~The Responsible Entity may choose to terminate routable protocol application sessions at a non-BES Cyber Asset inside the asset containing the low impact BES Cyber System(s) such that a separate application session is established to the low impact BES Cyber System(s) from the non-BES Cyber Asset (the routable session from outside the BES asset). The Responsible Entity may choose to authenticate access at a non-BES Cyber Asset either outside BES asset boundary or inside the asset containing the low impact BES Cyber System(s) such that unauthenticated access to the low impact BES Cyber System(s) is prohibited. The non-BES Cyber Asset sits on a demilitarized zone (DMZ) between the network outside the BES asset boundary and the low impact BES Cyber System(s). The non-BES Cyber Asset in the DMZ terminates the routable protocol session and establishes a new session to the low impact BES Cyber System(s). Additionally, a security device permits traffic from the network outside the BES asset boundary to flow only to and from the non-BES Cyber Asset in the DMZ (the routable session to the low impact BES Cyber System).~~



This reference model demonstrates that Responsible Entities have flexibility in choosing their electronic access controls so long as the security objective of the requirement is met. The

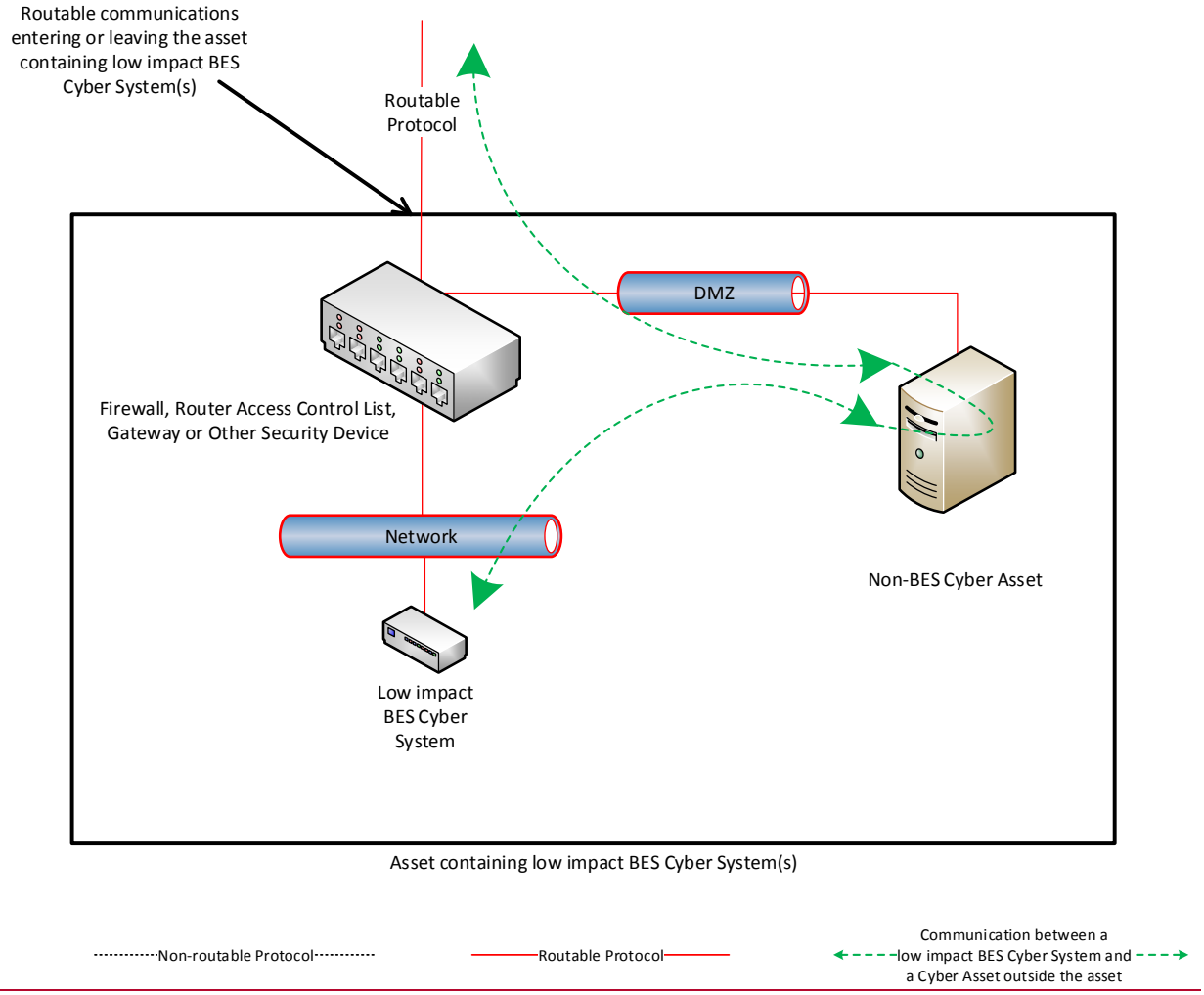
Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication must be configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications may be controlled in this network architecture by permitting no communication be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, the Responsible Entity needs to implement electronic access controls that permit only necessary inbound and outbound electronic access to the BES Cyber System. Consistent with the other reference models provided, this electronic access is controlled using the security device that is restricting the communication that is entering or leaving the asset.

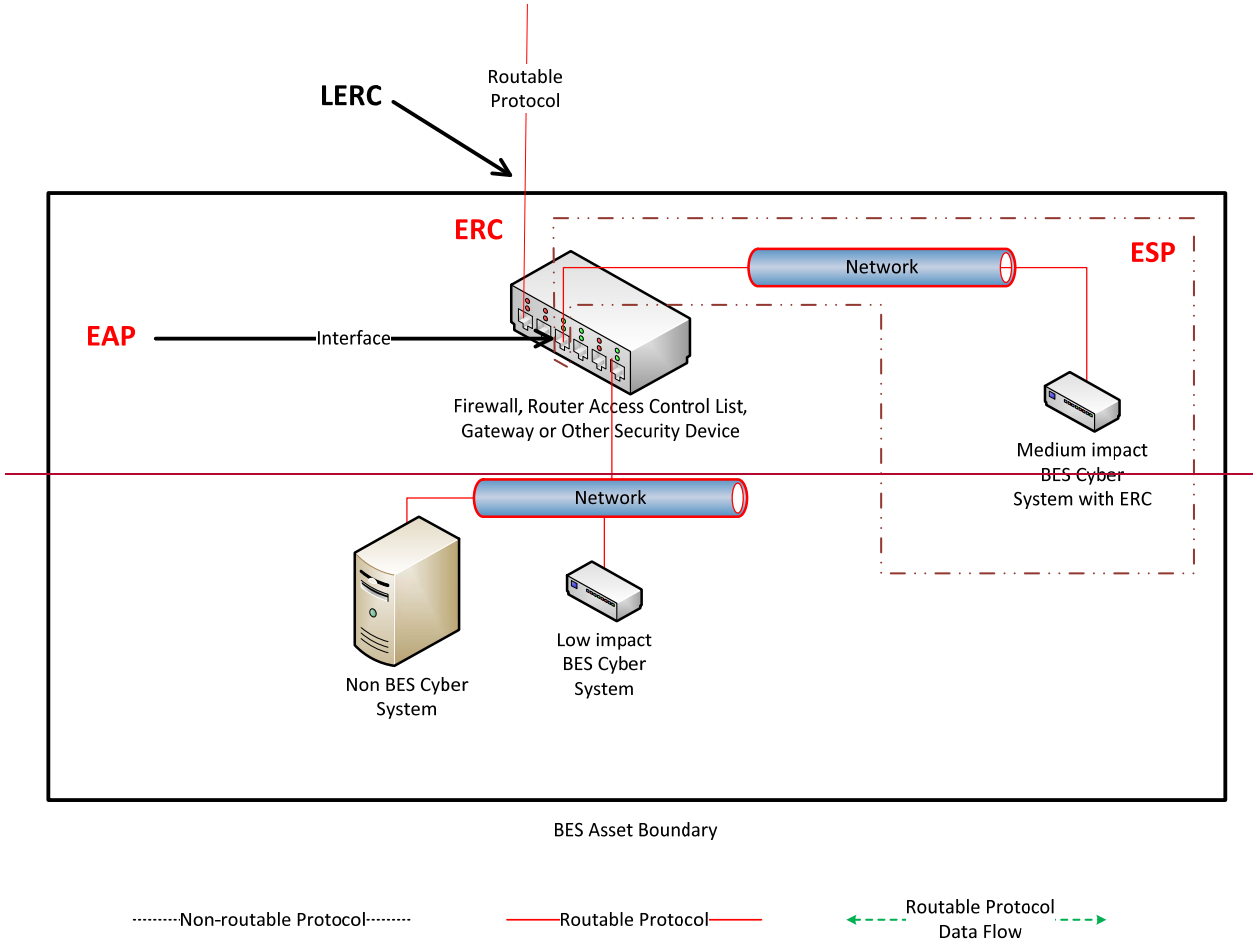


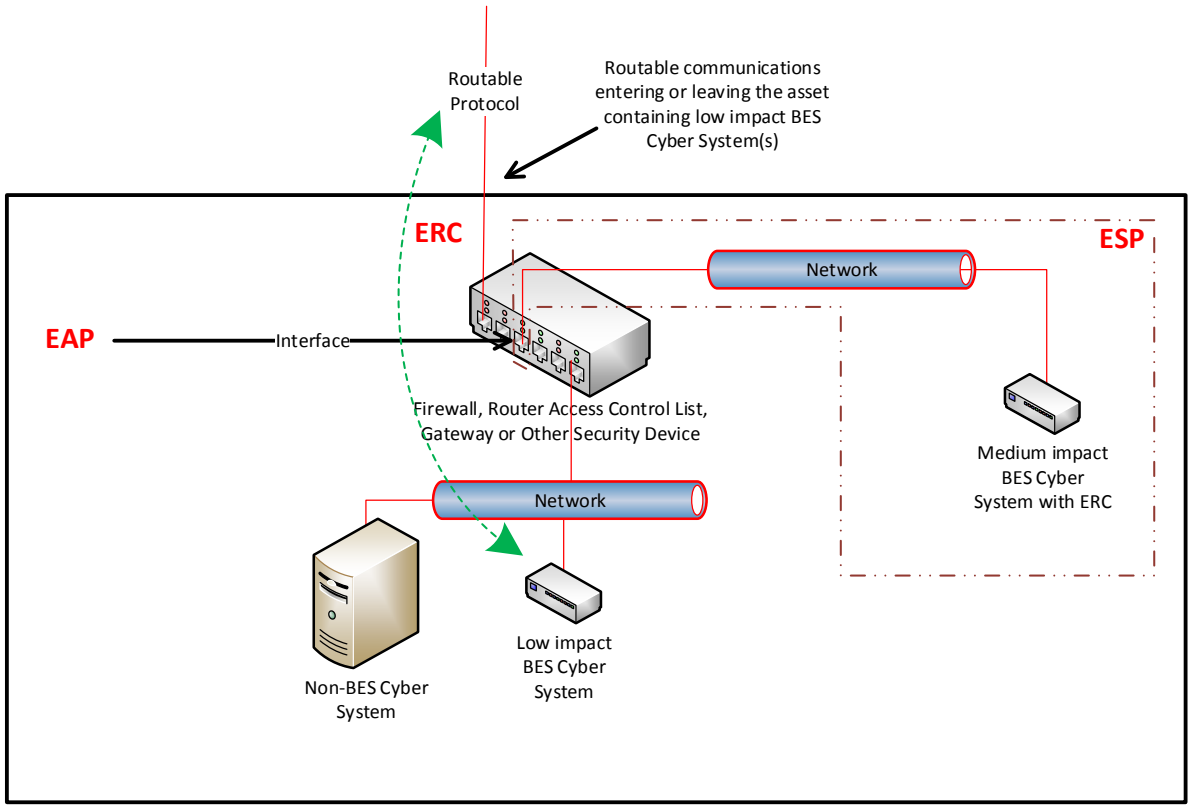
Reference Model 6

Reference Model ~~8~~

~~LERC Reference Model 9 – LERC~~7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

~~There is both LERC~~There is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and ERC present in this reference model because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the ~~BES asset.~~asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) ~~device~~ to provide electronic access controls ~~for the LERC~~. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing ~~low impact~~ electronic access controls for an asset containing low impact BES Cyber Systems.


LERC
Routable Protocol
ERC
ESP
Network
EAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Medium impact BES Cyber System with ERC
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary
Non-routable Protocol
Routable Protocol
Routable Protocol Data Flow



Reference Model ~~9~~7

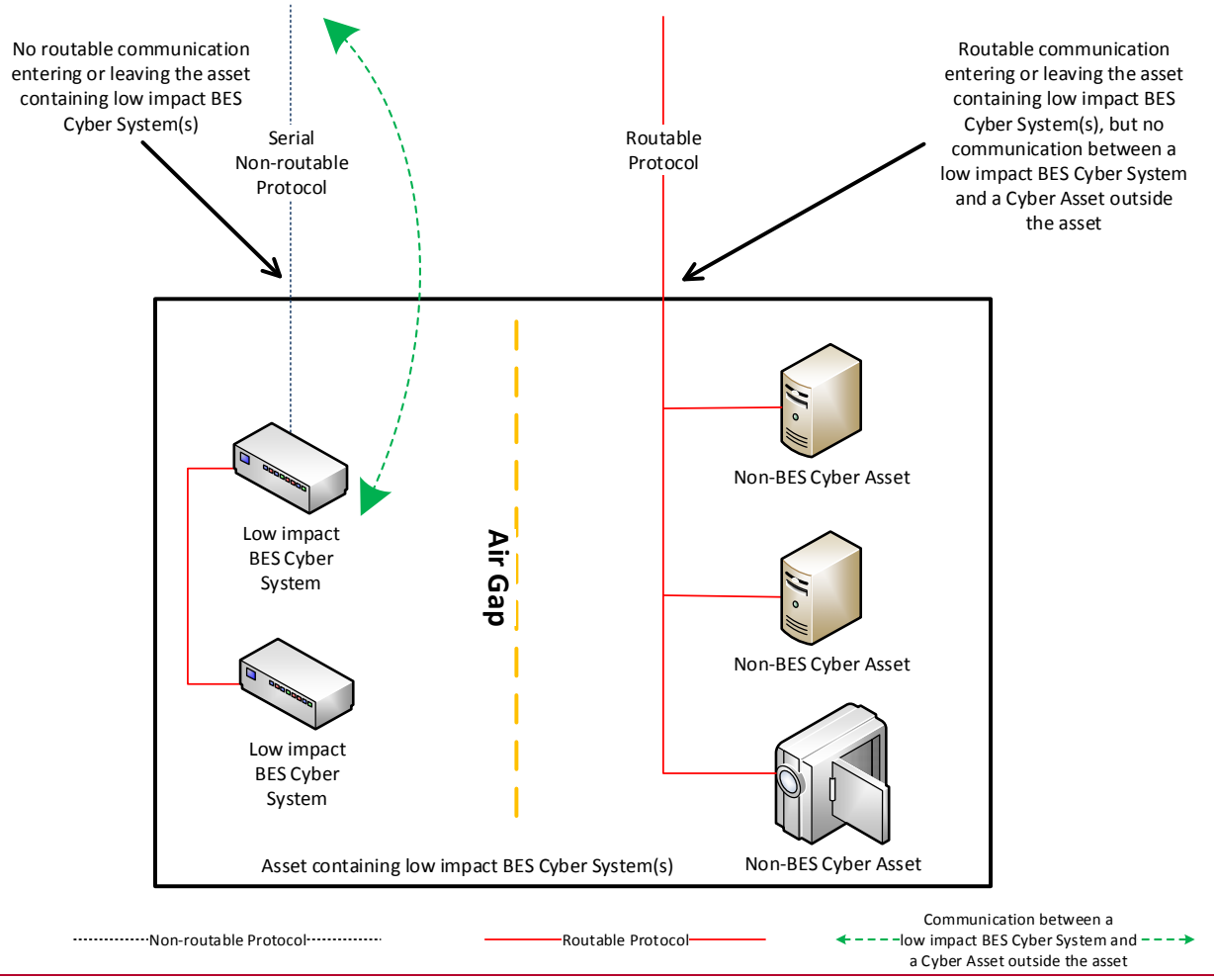
Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria for requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

1) physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;

2) communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls; and

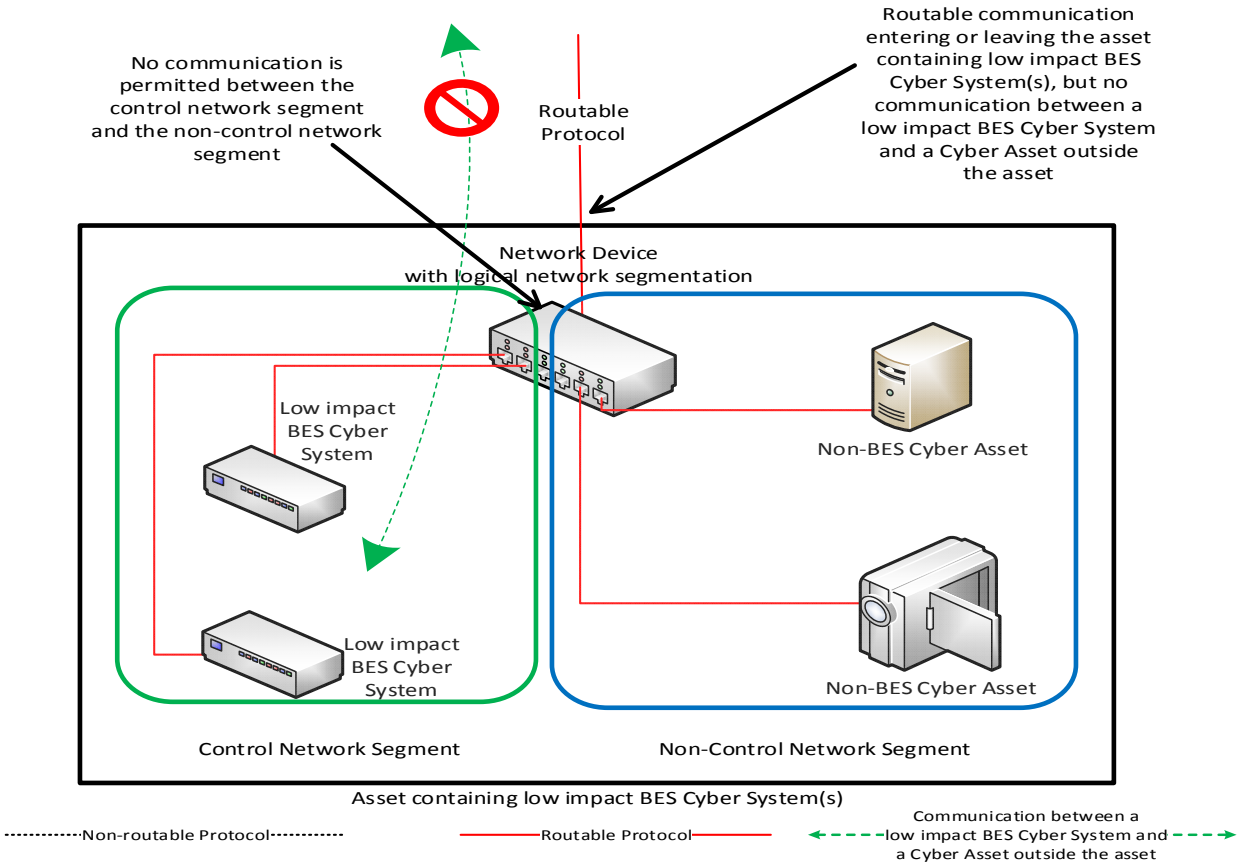
3) routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

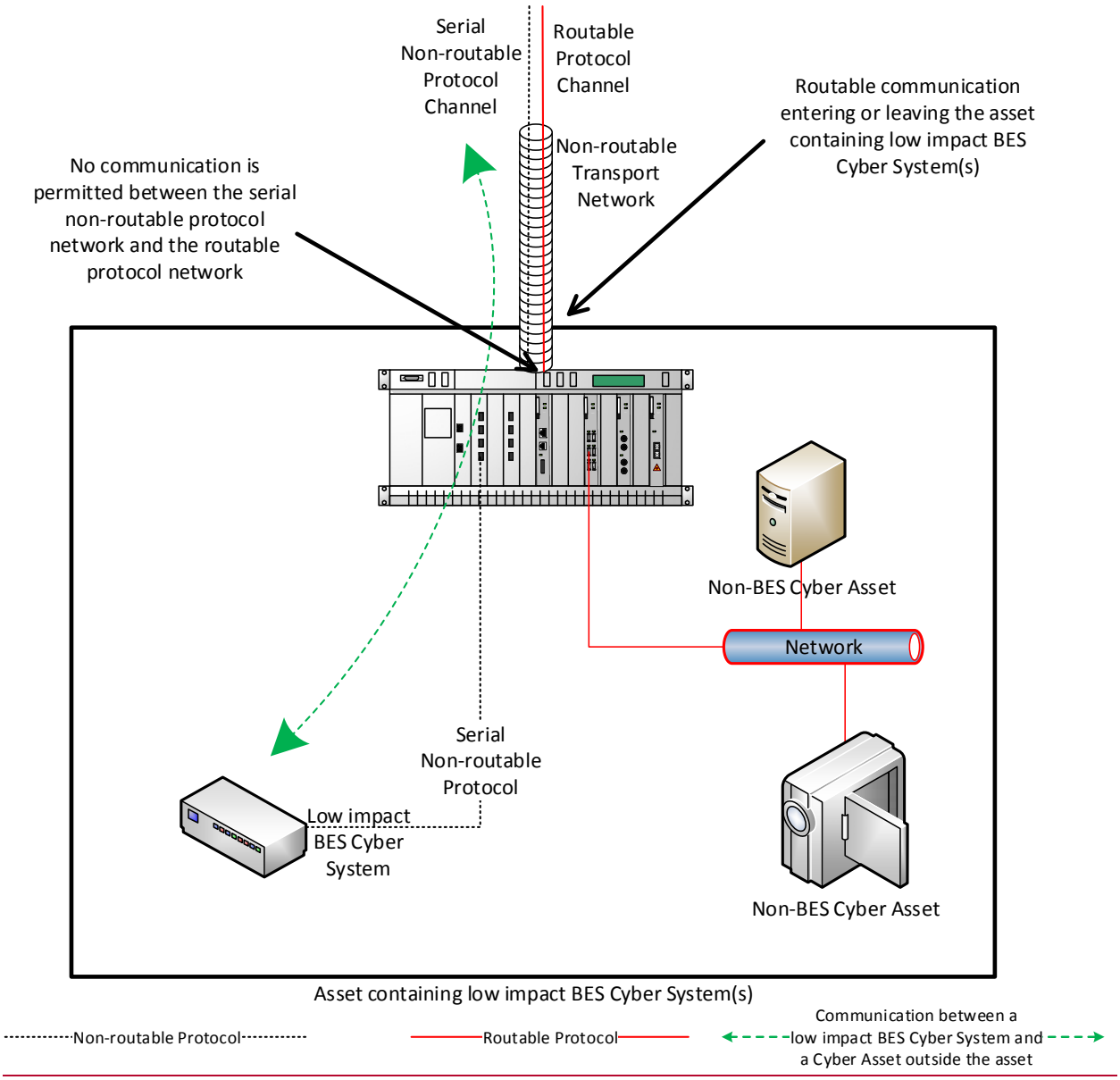
In this reference model, the criteria for requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a non-routable technology, such as a Time-Division Multiplexing (TDM) or Synchronous Optical (SONET) network. In this reference model, the criteria requiring electronic access controls are not met. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol. In similar configurations, the Responsible Entity should closely evaluate the transport entering or leaving the asset containing low impact BES Cyber System(s). If the communication entering or leaving the asset containing low impact BES Cyber System(s) was routable (such as serial encapsulated in TCP/IP or UDP/IP as depicted Reference Model 2 or Reference Model 5), then the criteria requiring electronic access controls would be met.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- ~~An asset has LERC due to a~~A low impact BES Cyber System ~~within it having~~has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

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.

Description of Current Draft

This draft of CIP-003-7 is addressing the directive issued by the Federal Energy Regulatory Commission (Commission) in paragraph 73 of Order No. 822 which reads:

> [T]he Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule approving revisions to the cybersecurity Critical Infrastructure Protection (CIP) standards.

In this revision, the SDT revised Sections 2 and 3 of Attachments 1 and 2 in CIP-003-7 and removed the terms *Low Impact External Routable Connectivity* (LERC) and *Low Impact BES Cyber System Electronic Access Point* (LEAP). The modifications incorporate concepts and select language from the LERC definition into Attachment 1, Section 3 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). The SDT simplified Section 3 of Attachment 1 to require the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the exclusion language (previously in the definition of LERC) contained in (iii) which reads: "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The defined term LEAP is no longer necessary because the SDT changed the requirement from requiring a LEAP to requiring electronic access controls. Additionally, since the SDT is removing the term LERC, the exclusion language that was previously in the definition of LERC was integrated into the Attachment 1, Section 3.1 requirement.

Because the proposed modifications to Reliability CIP-003-7 eliminate the need for the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP), NERC is requesting these terms be retired in the associated Implementation Plan.

Additionally, the SDT:

- revised the associated Lower, Moderate, and High VSLs for Requirement R2 to complement the requirement revisions;
- corrected a mistake in the Severe VSL for Requirement R2;
- made non-substantive changes to the Moderate and High VSLs for Requirement R2 to align with the order of the requirement;
- removed repetitive text from Requirement R1, Part 1.2.3 to make it consistent with Parts 1.2.1 and 1.2.2;
- updated the Guidelines and Technical Basis section of the standard to reflect the revisions made to the Attachments; and
- made non-substantive errata changes throughout the standard such as replacing "ES-ISAC" with "E-ISAC".

Completed Actions	Date
Standard Authorization Request (SAR) approved	July 20, 2016
Draft 1 of CIP-003-7 posted for formal comment and initial ballot	July 21 – September 6, 2016
Draft 2 of CIP-003-7 posted for formal comment and additional ballot	October 21 – December 5, 2016

Anticipated Actions	Date
10-day final ballot	January, 2017
NERC Board of Trustees (BOT) adoption	February, 2017
Petition filed with FERC	March, 2017

A. Introduction

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

2. **Number:** CIP-003-~~6~~7

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 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 SPS or RAS where the SPS or 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-~~6~~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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3 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.

4.2.3.4 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-~~6~~7.

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single

cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls ~~for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity~~; and

1.2.4. Cyber Security Incident response

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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but	The Responsible Entity failed to document ~~or~~and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to ~~CIP-003-6,~~ Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident	containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented	failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-67)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2)	its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification,	The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~E-ISAC) according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) ~~OR~~ ~~The Responsible Entity documented and implemented electronic access controls for LERC, but failed to implement a LEAP or permit inbound and outbound access according to CIP-003-6, Requirement R2,~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				classification, and response to Cyber Security Incidents according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) ~~-~~OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity ~~Sector~~ Information Sharing and Analysis Center	~~Attachment 1, Section 3.~~ ~~(R2)~~ ~~OR~~ ~~The Responsible Entity documented and implemented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to document and implement authentication of all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)~~ ~~OR~~ ~~The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-67)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(ESE-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4. OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to CIP-003-6, Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low	Systems, but failed to implement the physical security controls according to CIP-003-6, Requirement R2, Attachment 1, Section 2. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~impact BES Cyber Systems, but failed to document electronic access controls according to CIP-003-6, Requirement R2, Attachment 1, Section 3.~~ ~~(R2)~~		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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

Version	Date	Action	Change Tracking
			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 devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees.	Revised to address FERC Order 822 directive regarding definition of LERC.

Attachment 1

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

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

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

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

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security control objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition…within one year of the effective date of this Final Rule.

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the exclusion language (previously in the definition of LERC) contained in (iii) which reads: "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The

focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

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

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

Section 3. ~~For LERC, if any,~~ implement ~~a LEAP to permit~~electronic access controls to:

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

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

~~i.~~ii. using a routable protocol ~~access; and~~when entering or leaving the asset containing the low impact BES Cyber System(s); and,

iii. ~~Implement authentication for~~not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~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.

~~CIP-003-6~~ Attachment 2

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

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

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

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

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

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

1. ~~Documentation showing that inbound and outbound connections for any LEAP(s) are confined to only those the Responsible Entity deems necessary (e.g., by restricting IP addresses, ports, or services); and documentation~~Documentation, such as representative diagrams or lists of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; implementing unidirectional gateways) showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices; and

~~1.~~2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems

that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~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.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-~~6~~7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-~~6~~7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-~~6~~7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts

- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

~~Using the list of assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement~~The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that ~~addresses~~address the security objective ~~criteria~~ for the protection of low impact BES Cyber Systems. ~~The protections required by Requirement R2 reflect the level of risk that misuse or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the~~The required protections are designed to

be part of a program that covers the low impact BES Cyber Systems collectively ~~either~~ at an asset ~~or site~~ level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

~~There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and~~

~~**Dial-up Connectivity**, and (4) Cyber Security Incident response.~~

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the ~~four~~ subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The Responsible Entity is not required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems ~~at assets containing low impact BES Cyber System(s)~~ within the asset, and (2) ~~LEAPs~~Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Section 3.1, if any. If ~~the LEAP is~~these Cyber Assets implementing the electronic access controls are located within the ~~BES asset~~ same asset as the low impact BES Cyber Asset(s) and ~~inherits~~inherit the same physical access controls outlined in Section 2, this can be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility ~~in the selection of~~to select the methods used to meet the objective ~~to control~~ of controlling physical access to (1) the asset(s) containing low impact BES Cyber ~~Systems,~~System(s) or the low impact BES Cyber Systems themselves~~, or LEAPs~~ and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The

Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level for access to the site or systems, including LEAPs.. The requirement does not obligate an entity to specify a need for each physical access or authorization of a useran individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of boundary protectionselectronic access controls for assets containing low impact BES Cyber Systems when the low impact BES Cyber Systems have bi-directionalthere is routable protocol communication or Dial-up Connectivity to devices external to between Cyber Asset(s) outside of the asset containing the low impact BES Cyber Systems. The establishment of boundary protections is intended to control communication either into the asset containing low impact BES Cyber System(s) or toand the low impact BES Cyber System itself to (s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. The term "electronic access control" is used in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing. The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or Dial-up Connectivity present. In the case where there is no external bi-directional routable protocol communication or Dial-up Connectivity, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s).

The defined terms LERCWhen implementing Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and LEAPoutbound electronic access are used to avoid confusion with the similar terms usedrequired for highcommunications when those communications meet all three of the criteria identified in Section 3.1. The

Responsible Entity should evaluate the communications and mediumwhen all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems (e.g., External Routablethat use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, Responsible Entities are to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity (ERC) or to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, any communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), does not require evaluation for electronic access controls.

Electronic Access Point (EAP)). To future-proof the standards, and inControl Exclusion

In order to avoid future technology issues, the definitions specificallyobligations for electronic access controls exclude "point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems,", such as IEC TR-61850-90-5 R-GOOSE messaging. This does not exclude Control Center communication but rather excludes the communication between the intelligent electronic devices themselves.Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement a LEAP.the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive requirementscharacteristics related to this technology norand not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

When determining whether **Considerations for Determining Routable Protocol Communications**

In order for Responsible Entities to determine whether electronic access controls need to be implemented, the Responsible Entity needs to determine whether there is LERC to the low impact BES Cyber System, the definition uses the phrases "direct user-initiated interactive access or a direct device-to-device connection to communication between a low impact BES Cyber System(s) fromand a Cyber Asset(s) outside the asset containing thosethe low impact BES Cyber System(s) viathat use a routable protocol when entering or leaving the asset.

When determining whether a bi-directional routable protocol connection." The intent of "direct" in the definition is to indicate LERC exists if a person is sitting at another device outside ofentering or leaving the asset containing the low impact BES Cyber System, and (s), Responsible Entities have flexibility in identifying an approach to making this evaluation. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session even if there is a serial to routable protocol conversion. The reverse case would also be LERC, in which the individual sits at thecommunication entering or leaving the asset between a low impact BES Cyber System and connectsCyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to a device the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for "device to System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the Responsible Entity documents and implements its chosen electronic access control(s). The control(s) must allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. The Responsible Entity must be able to explain the reasons for the electronic access permitted. The reasoning for the

"necessary" inbound and outbound electronic access controls can be documented within the Responsible Entity's cyber security plan(s) or other policies or procedures associated with the electronic access controls.

Concept Diagrams

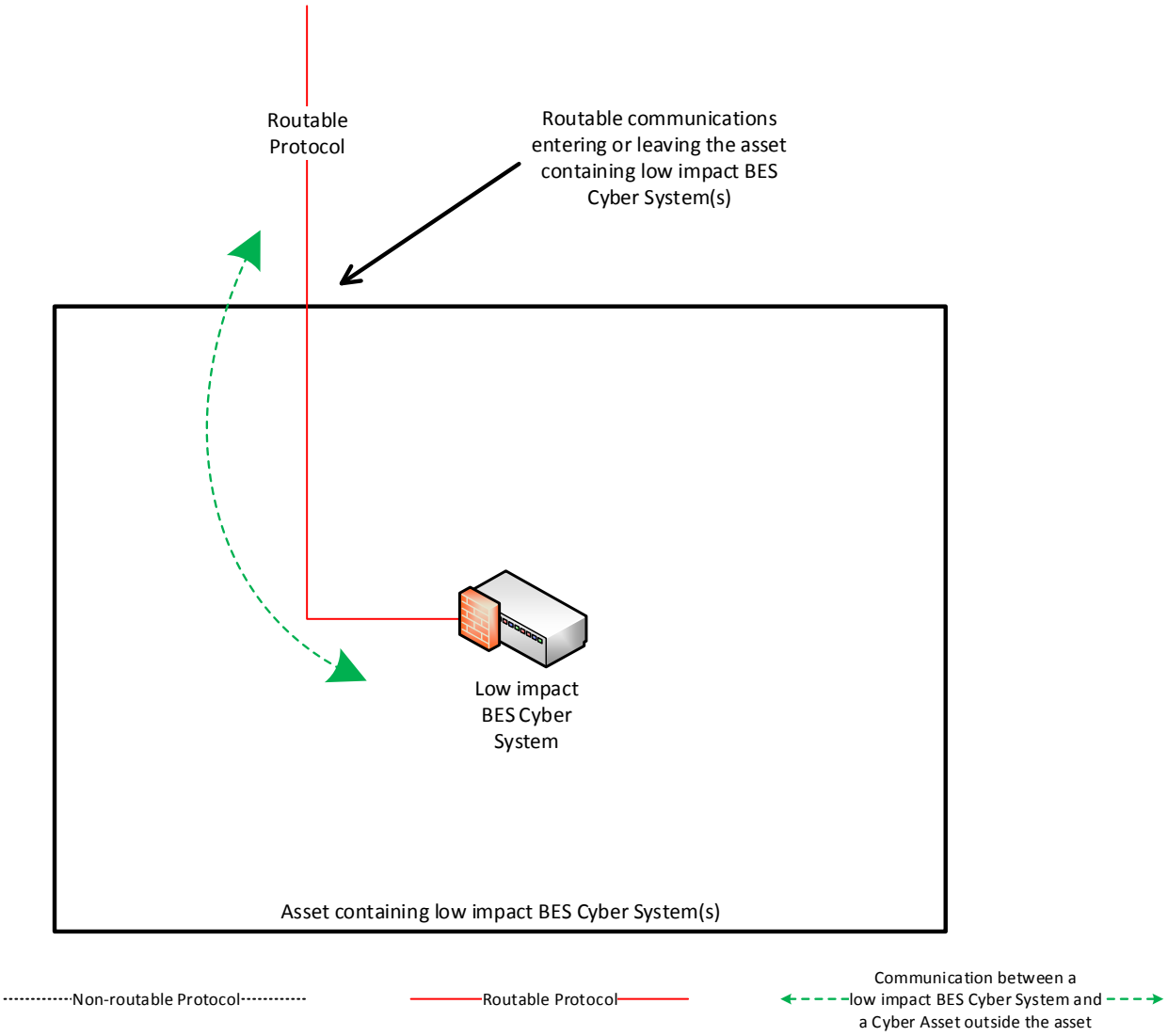
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset must be met.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

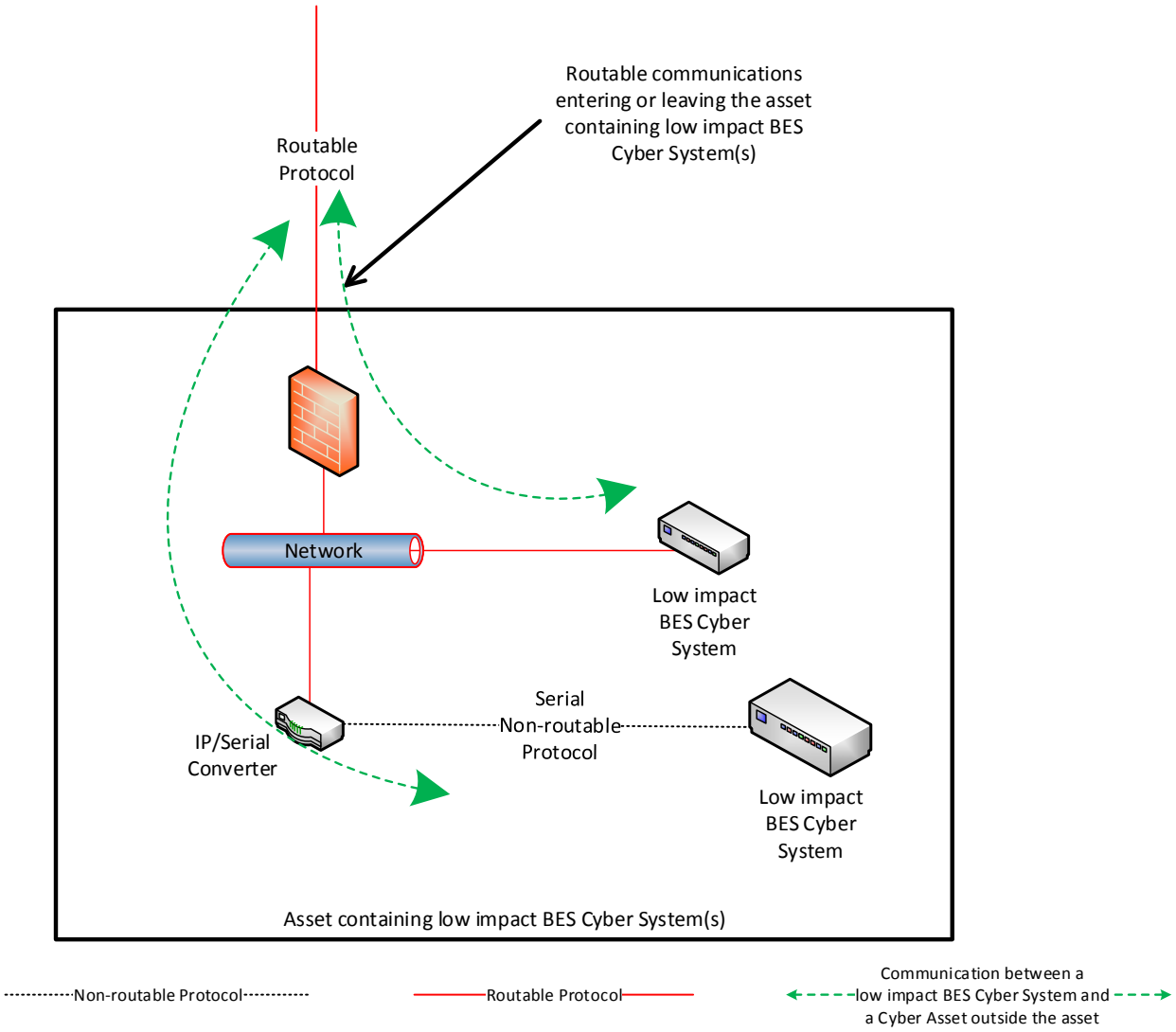
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound routable protocol access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary. Responsible Entities may further restrict electronic access using ports and services based on the capability of the electronic access control, low impact BES Cyber System, application, etc.



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

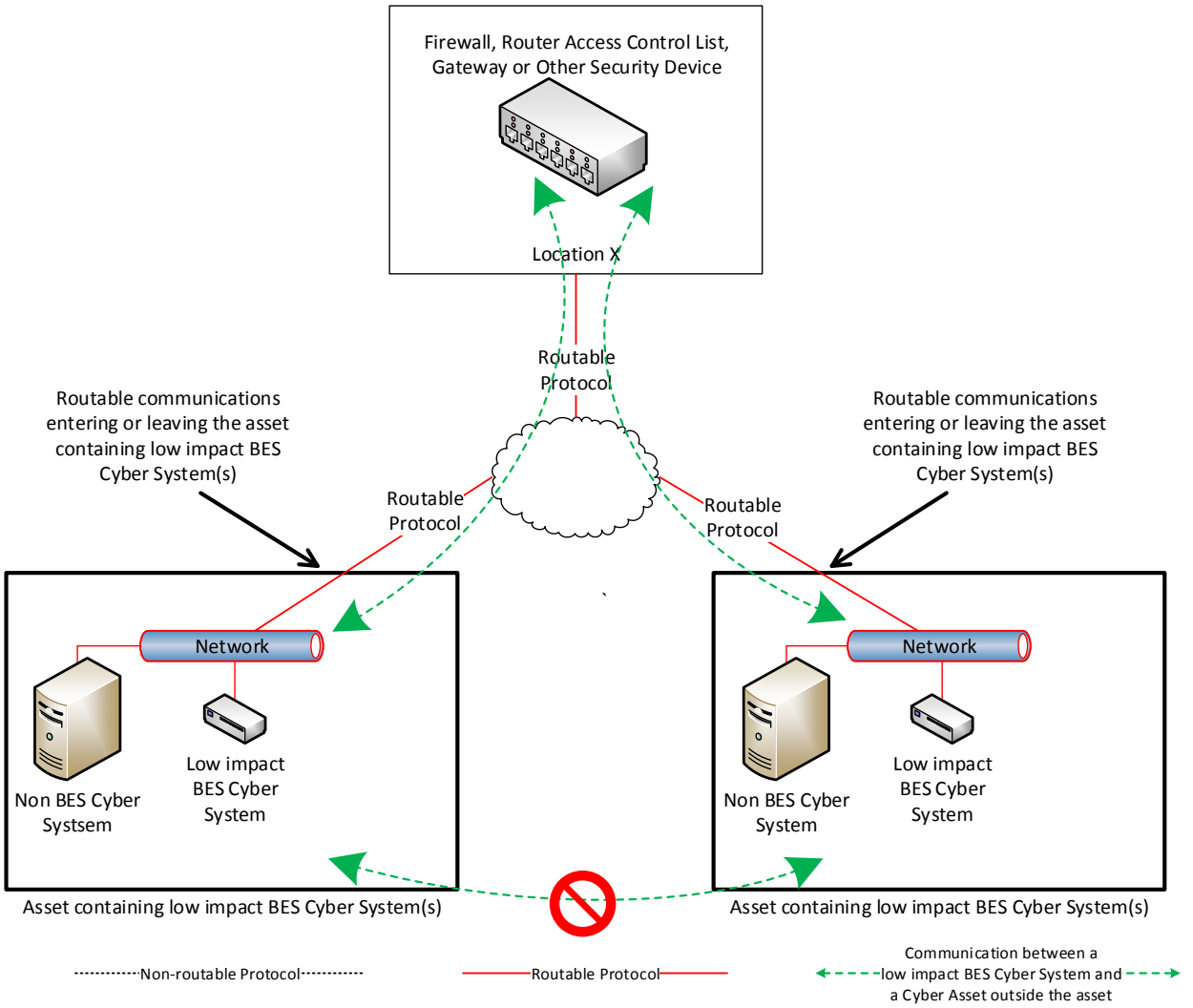
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary. Responsible Entities may further restrict electronic access using ports and services based on the capability of the electronic access control, low impact BES Cyber System, application, etc.



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

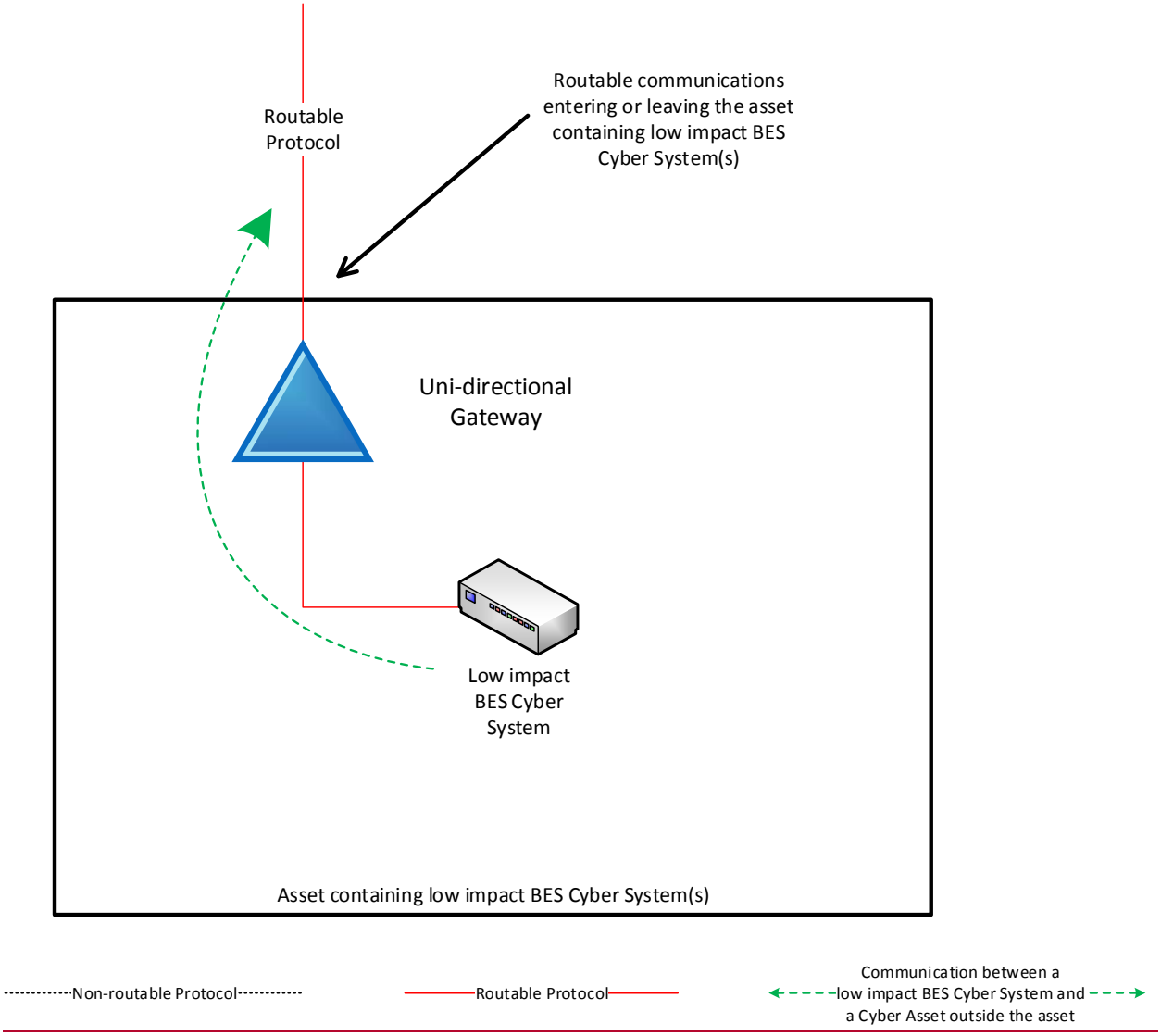
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary. Responsible Entities can further restrict electronic access using ports and services based on the capability of the electronic access control, low impact BES Cyber System, application, etc.



Reference Model 3

Reference Model 4 – Uni-directional Gateway

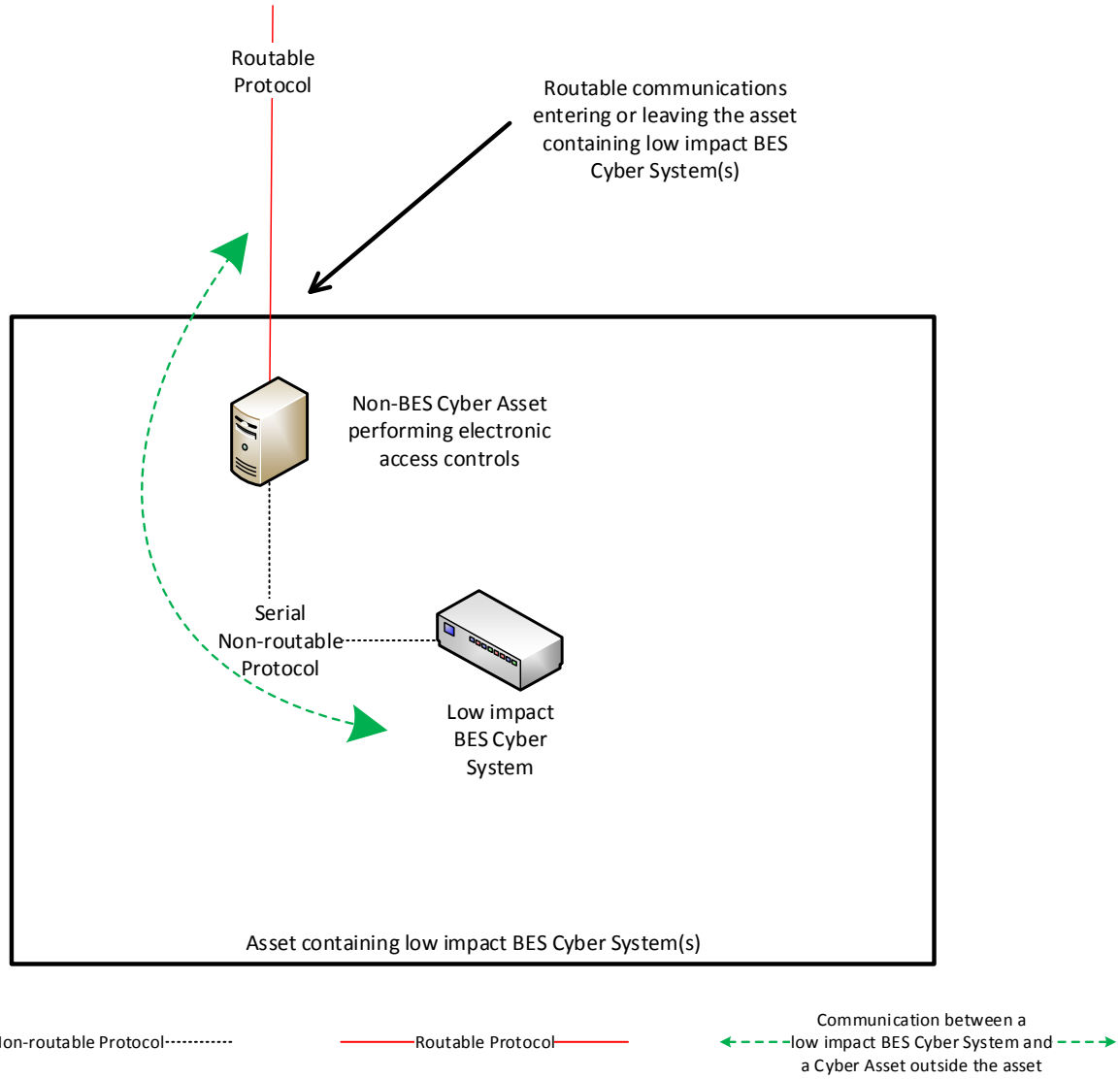
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

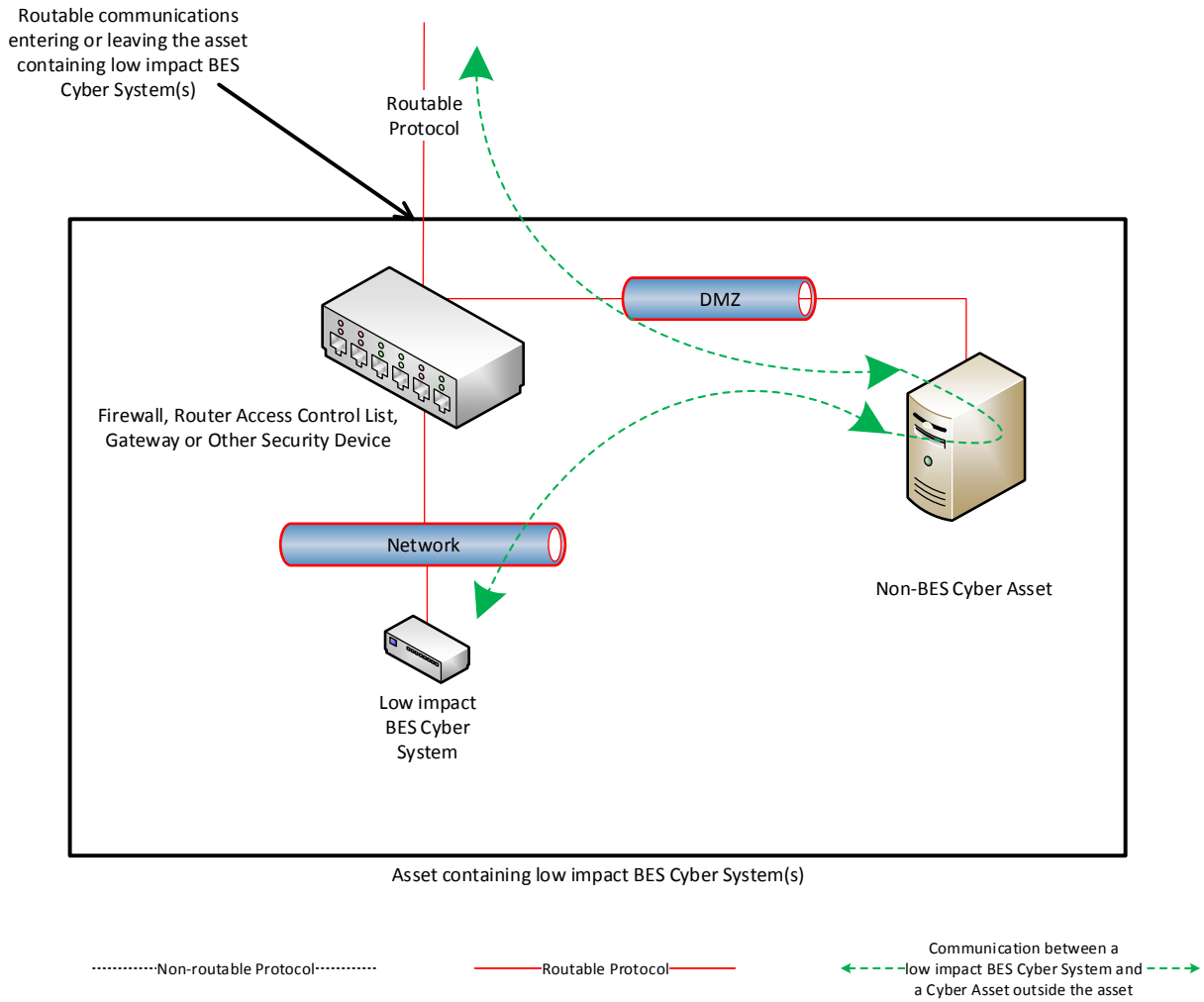
This reference model demonstrates that Responsible Entities have flexibility in choosing their electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication must be configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications may be controlled in this network architecture by permitting no communication be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

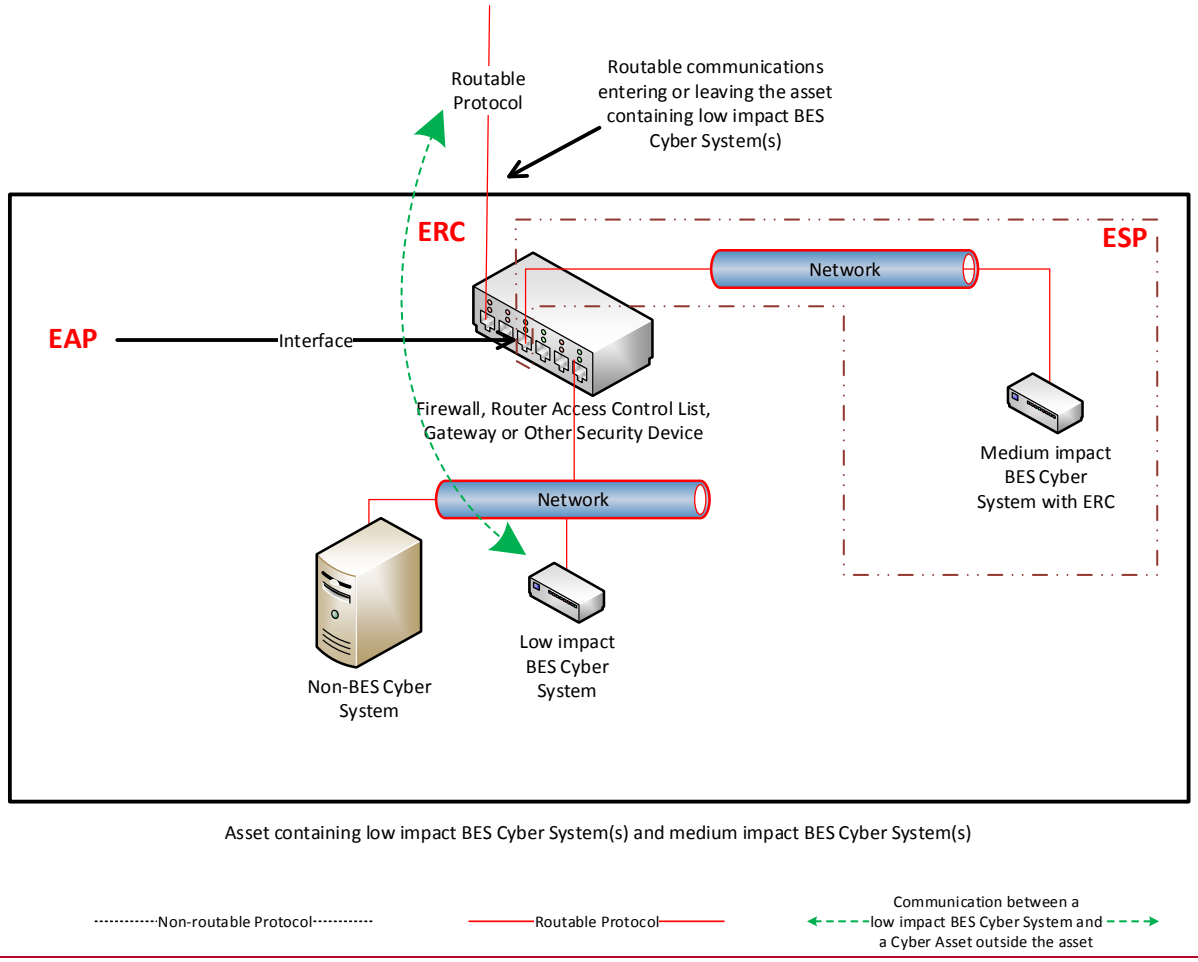
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, the Responsible Entity needs to implement electronic access controls that permit only necessary inbound and outbound electronic access to the BES Cyber System. Consistent with the other reference models provided, this electronic access is controlled using the security device ~~connection," LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication to or from the low impact BES Cyber System.~~ that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

There is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and ERC present in this reference model because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.



Reference Model 7

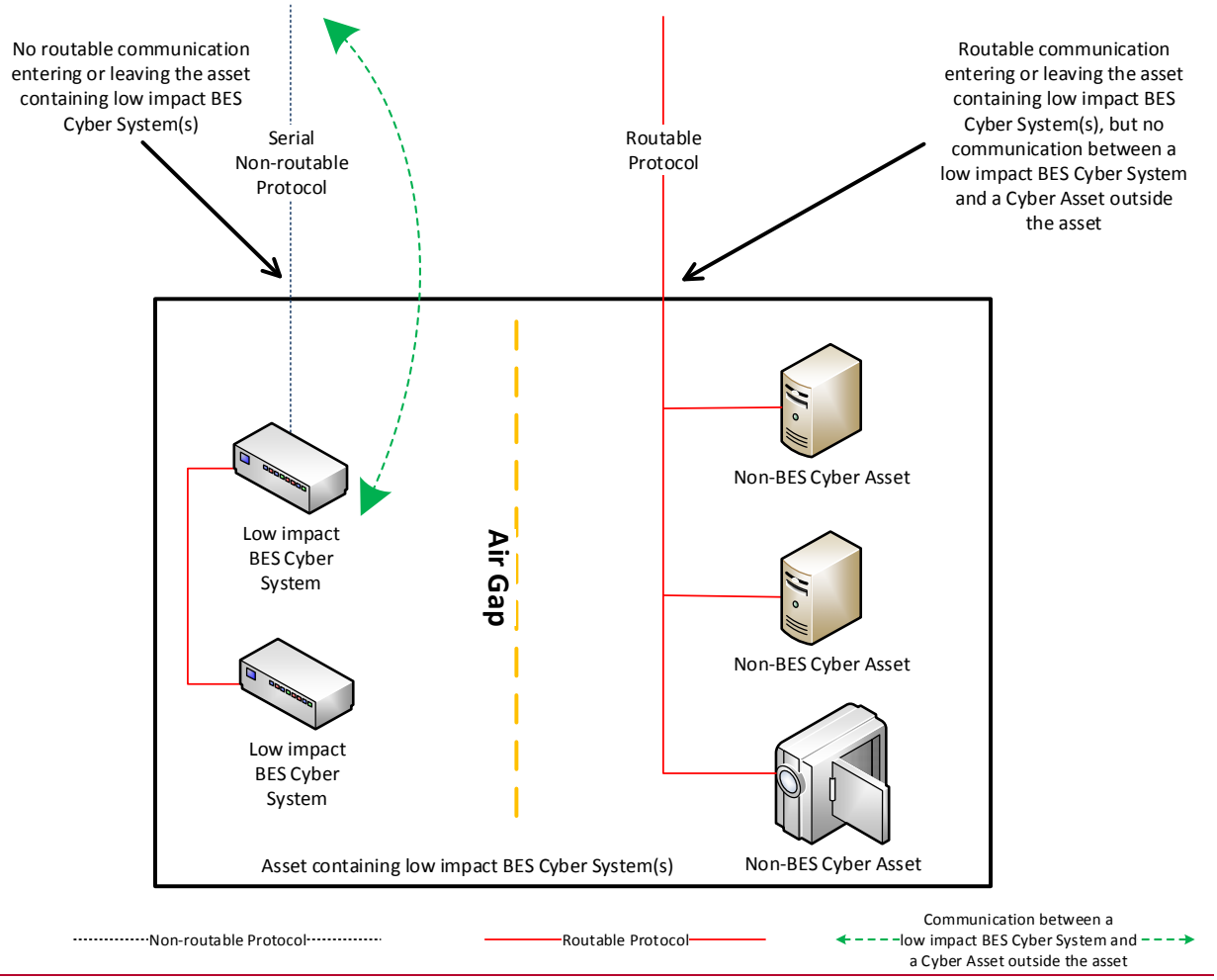
Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria for requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

1) physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;

2) communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls; and

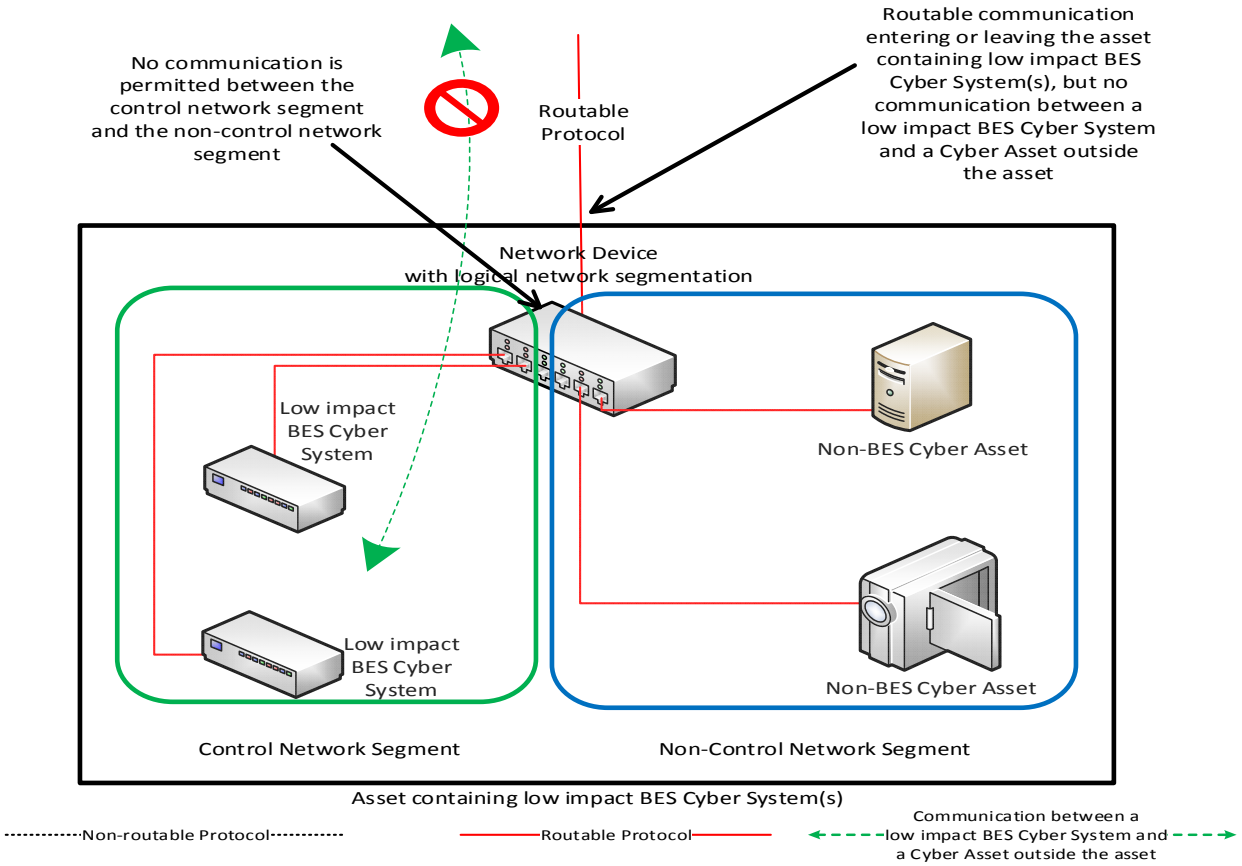
3) routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

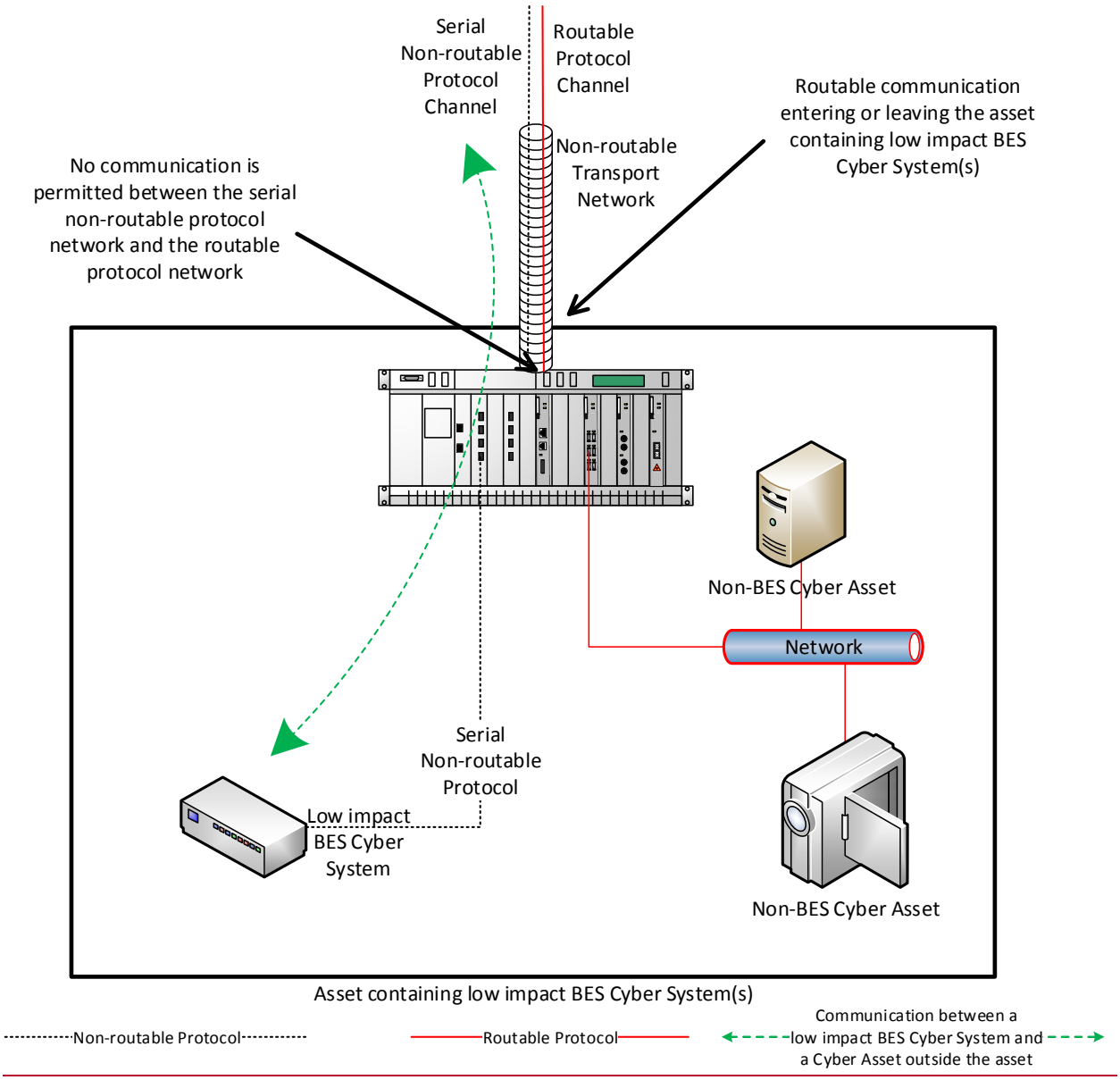
In this reference model, the criteria for requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a non-routable technology, such as a Time-Division Multiplexing (TDM) or Synchronous Optical (SONET) network. In this reference model, the criteria requiring electronic access controls are not met. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol. In similar configurations, the Responsible Entity should closely evaluate the transport entering or leaving the asset containing low impact BES Cyber System(s). If the communication entering or leaving the asset containing low impact BES Cyber System(s) was routable (such as serial encapsulated in TCP/IP or UDP/IP as depicted Reference Model 2 or Reference Model 5), then the criteria requiring electronic access controls would be met.



Reference Model 10

Dial-up Connectivity When identifying a LEAP, Responsible Entities are provided flexibility in the selection of the interface on a Cyber Asset that controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, the internal interface on a router that has implemented an access control list (ACL), or other security device. The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required to reside at the asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP per asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber Systems. Locating the Cyber Asset with multiple LEAPs at an external location with multiple assets containing low impact BES Cyber Systems "behind" it, however, should not allow uncontrolled access to assets containing low impact BES Cyber Systems sharing a Cyber Asset containing the LEAP(s).

In Reference Model 4, the communication flows through an IP/Serial converter. LERC is correctly identified in this Reference Model because the IP/Serial converter in this instance is doing nothing more than extending the communication between the low impact BES Cyber System and the Cyber Asset outside the asset containing the low impact BES Cyber System. In contrast, Reference Model 6 has placed a Cyber Asset that performs a complete break or interruption that does not allow the user or device data flow to directly communicate with the low impact BES Cyber System. The Cyber Asset in Reference Model 6 is preventing extending access to the low impact BES Cyber System from the Cyber Asset outside the asset containing the low impact BES Cyber System. The intent is that if the IP/Serial converter that is deployed only does a "pass-through" of the data flow communication, then that "pass-through" data flow communication is LERC and a LEAP is required. However, if that IP/Serial converter performs some type of authentication in the data flow at the asset containing the low impact BES Cyber System before the communication can be sent to the low impact BES Cyber System, then that type of IP/Serial converter implementation is not LERC.

A Cyber Asset that contains interface(s) that only perform the function of a LEAP does not meet the definition of Electronic Access Control or Monitoring System (EACMS) associated with medium or high impact BES Cyber Systems and is not subject to the requirements applicable to an EACMS. However, a Cyber Asset may contain some interfaces that function as a LEAP and other interfaces that function as an EAP for high or medium impact BES Cyber Systems. In this case, the Cyber Asset would also be subject to the requirements applicable to the EACMS associated with the medium or high impact BES Cyber Systems.

Examples of sufficient access controls may include:

- Any LERC for the asset passes through a LEAP with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g., IP addresses, ports, or services).
- As shown in Reference Model 1 below, the low impact BES Cyber System has a host-based firewall that is controlling the inbound and outbound access. In this model, it is also possible that the host-based firewall could be on a non-BES

Cyber Asset. The intent is that the host-based firewall controls the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in the business network.

- As shown in Reference Model 5 below, a non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that the non-BES Cyber Asset has provided a "protocol break" so that access to the low impact BES Cyber System is only from the non-BES Cyber Asset that is located within the asset containing the low impact BES Cyber System.

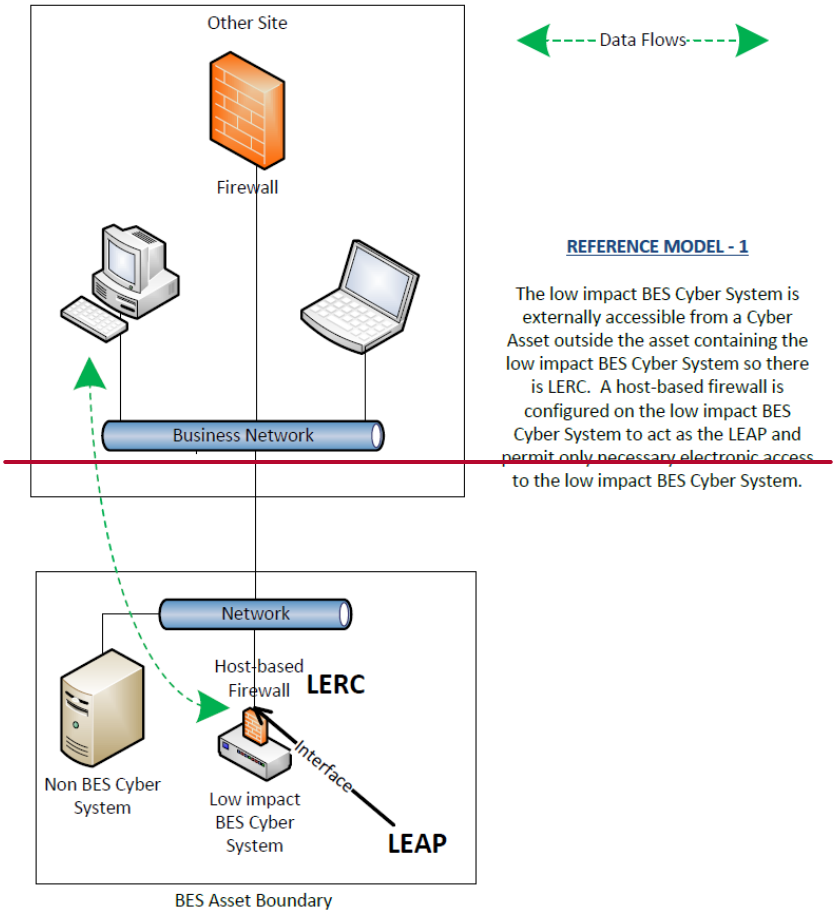
Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

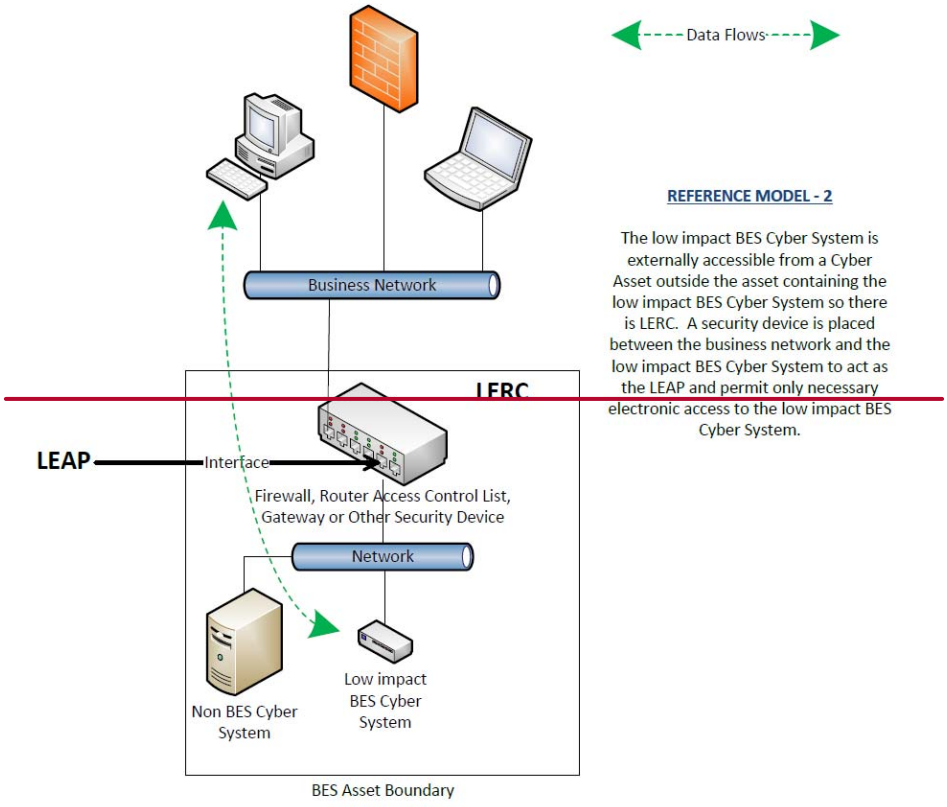
Insufficient Access Controls

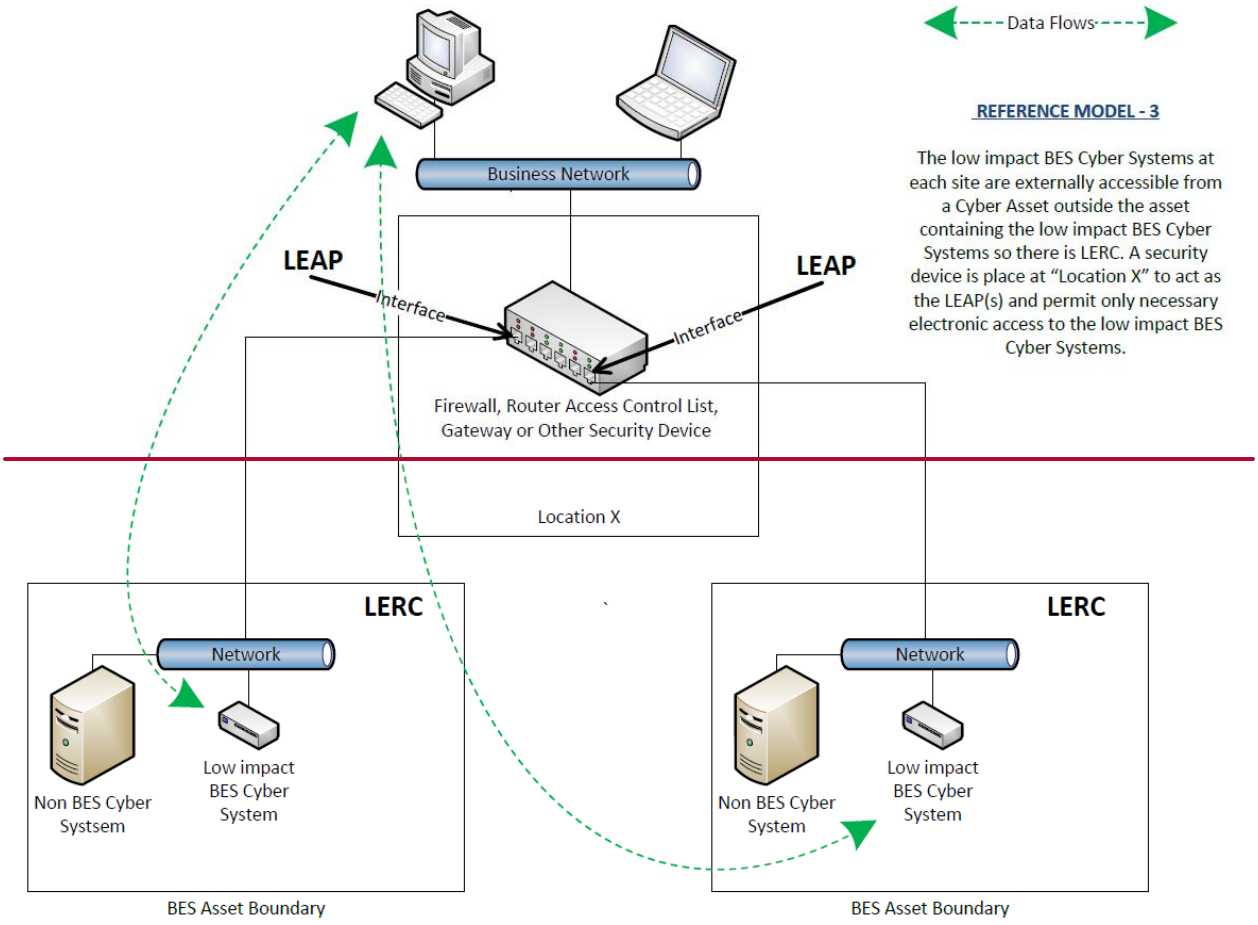
Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

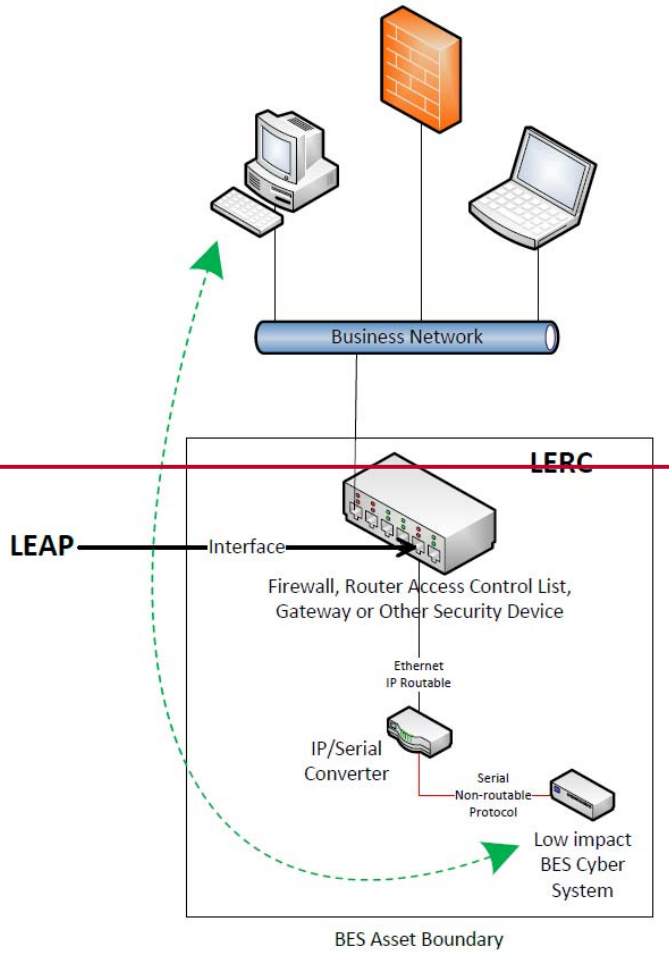
- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- An asset has LERC due to aA low impact BES Cyber System within it havinghas a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- In Reference Model 5, using just dualDual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the businessexternal network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devicedevices on thatthe non-BES Cyber Asset.

The following diagrams provide reference examples intended to illustrate how to determine whether there is LERC and for implementing a LEAP. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.


Other Site
Data Flows
Firewall
Business Network
REFERENCE MODEL - 1
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A host-based firewall is configured on the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.
Network
Host-based Firewall
LERC
Interface
Non BES Cyber System
Low impact BES Cyber System
LEAP
BES Asset Boundary


Data Flows
REFERENCE MODEL - 2
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.
Business Network
LERC
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

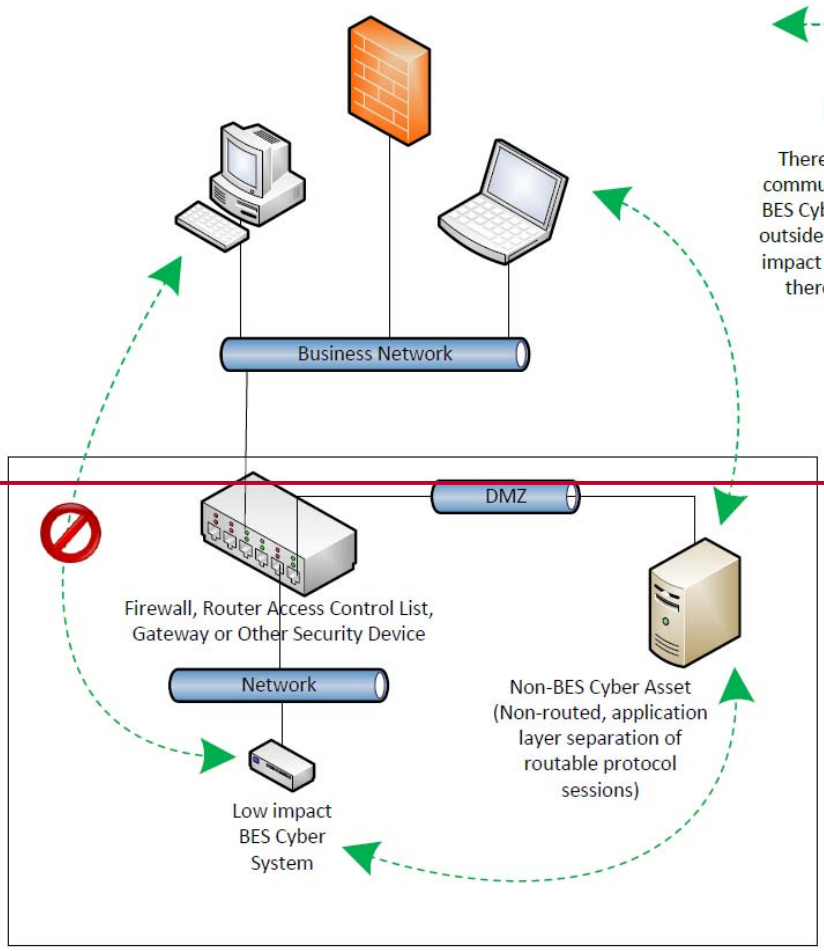

Data Flows
REFERENCE MODEL - 3
The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is place at "Location X" to act as the LEAP(s) and permit only necessary electronic access to the low impact BES Cyber Systems.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Location X
LERC
Network
Non BES Cyber Systsem
Low impact BES Cyber System
BES Asset Boundary
LERC
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

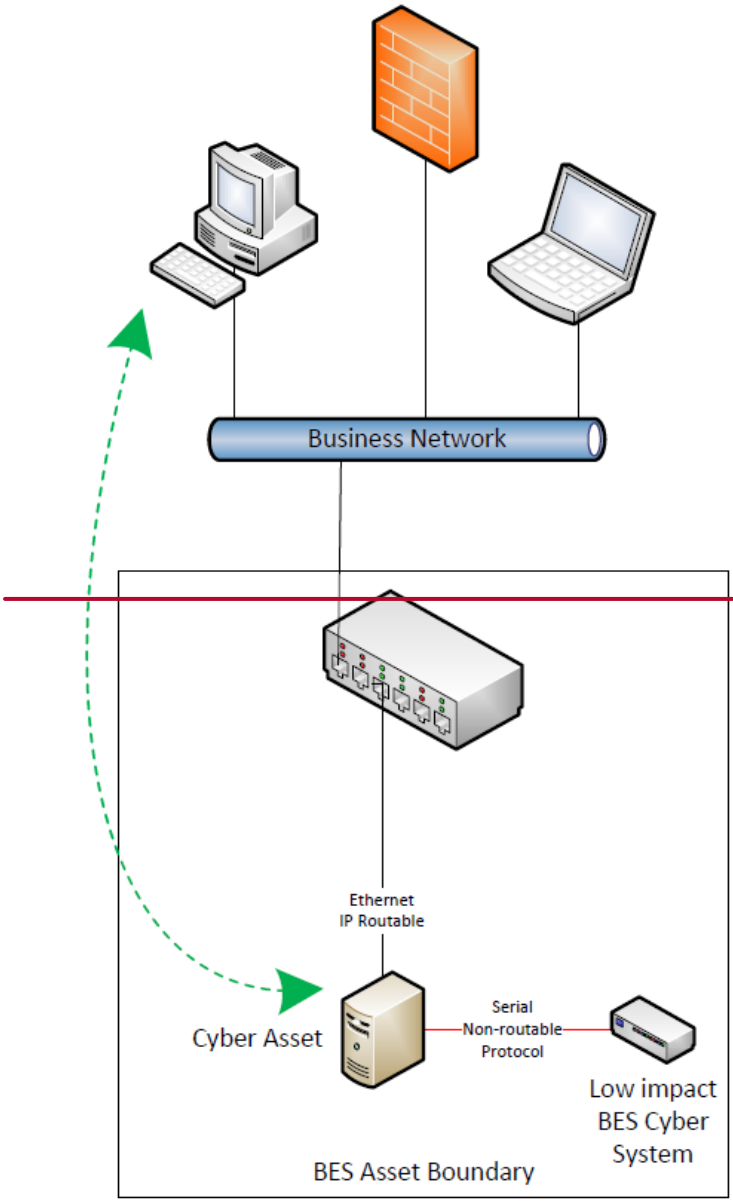


Data Flows

REFERENCE MODEL - 4

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.

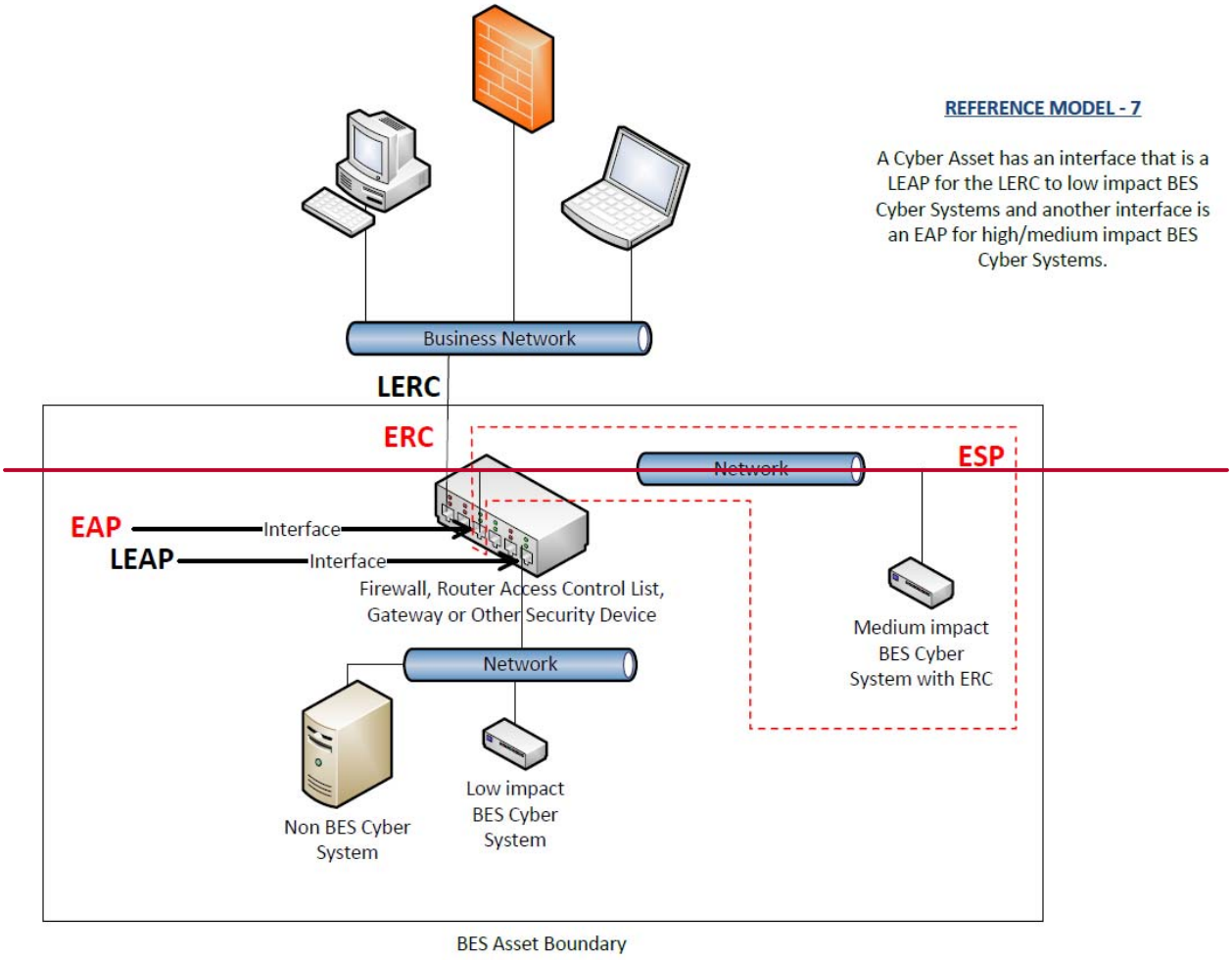

Data Flows
REFERENCE MODEL - 5
There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.
Business Network
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset (Non-routed, application layer separation of routable protocol sessions)
Low impact BES Cyber System
BES Asset Boundary



Data Flows

REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.



Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident

counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-~~6~~7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-~~6~~7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for

responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-003-7 Security Management Controls and Low Impact External Routable Communication (LERC)

Requested Approvals

- Reliability Standard CIP-003-7 - Cyber Security – Security Management Controls

Requested Retirements

- Reliability Standard CIP-003-6 - Cyber Security – Security Management Controls
- Definition Low Impact BES Cyber System Electronic Access Point (LEAP)
- Definition of Low Impact External Routable Connectivity (LERC)

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards,* approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions. In addition to approving the seven CIP Reliability Standards, the Commission, among other things, directed NERC to modify the definition of LERC. The Commission stated:

> 73. Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity

definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

As an alternative to modifying the definition consistent with the Commission's directive, the standard drafting team retired the term "LERC" and incorpored the LERC concepts within the requirement language.

Given the proposed retirement of the LERC definition and the proposed modifications in Reliability Standard CIP-003-7, there is no longer a need for the NERC Glossary term Low Impact BES Cyber System Electronic Access Point (LEAP). Consequently, NERC is proposing to retire the term LEAP.

General Considerations

The effective dates or phased-in compliance dates within the CIP-003-6 Implementation Plan, remain in effect except that the compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7.

The Responsible Entity shall not be required to include in its cyber security plan(s) elements related to Sections 2 and 3 of Attachment 1 until the effective date of CIP-003-7. Upon the effective date of CIP-003-7, the Responsible Entity's cyber security plan(s) must include the elements required by Sections 2 and 3 of Attachment 1 and the Responsible Entity must implement the controls included in its plan to meet the objectives of Sections 2 and 3.

Effective Date

The effective date for the proposed Reliability Standard is provided below:

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7 shall become effective on the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-7 shall become effective on the first day of the first calendar quarter that is twelve (12) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Planned or Unplanned Changes

Planned or Unplanned Changes Resulting in a Higher Categorization – This implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-5 titled Planned or Unplanned Changes Resulting in a Higher Categorization.[1]

Unplanned Changes Resulting in Low Impact Categorization – This implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-6 titled Unplanned Changes Resulting in Low Impact Categorization. That section provides:

> For unplanned changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

Retirement Date

Reliability Standard CIP-003-6

Reliability Standard CIP-003-6 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-7 in the particular jurisdiction in which the revised standard is becoming effective.

Current NERC Glossary of Terms of LERC and LEAP

The current definition of LERC and the term LEAP shall be retired from the NERC Glossary of Terms immediately prior to the effective date of CIP-003-7 in the particular jurisdiction in which the definition is becoming effective.

[1] Due to the length of that section, it is not reproduced herein.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-003-7 Security Management Controls and Low Impact External Routable Communication (LERC)

Requested Approvals

- Reliability Standard CIP-003-7 - Cyber Security – Security Management Controls
- ~~Definition of Low Impact External Routable Communication (LERC)~~

Requested Retirements

- Reliability Standard CIP-003-6 - Cyber Security – Security Management Controls
- Definition Low Impact BES Cyber System Electronic Access Point (LEAP)
- Definition of Low Impact External Routable Connectivity (LERC)

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards,* approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions. In addition to approving the seven CIP Reliability Standards, the Commission, among other things, directed NERC to modify the definition of LERC. The Commission stated:

> 73. Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity

definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

~~In addition~~As an alternative to modifying the definition consistent with the Commission's directive, the standard drafting team ~~revised the term "LERC" by replacing the word "connectivity" with the word "communication" such that the proposed term for inclusion in the Glossary of Terms used in NERC Reliability Standards (NERC Glossary) is "Low Impact External Routable Communication."~~retired the term "LERC" and incorpored the LERC concepts within the requirement language.

Given the ~~modified~~ proposed retirement of the LERC definition ~~of LERC~~ and the proposed modifications in Reliability Standard CIP-003-7, there is no longer a need for the NERC Glossary term Low Impact BES Cyber System Electronic Access Point (LEAP). Consequently, NERC is proposing to retire the term LEAP.

General Considerations

~~This Implementation Plan does not modify the~~ The effective ~~date for~~ dates or phased-in compliance dates within the CIP-003-6 ~~in the~~ Implementation Plan ~~associated with CIP-003-6 nor any of~~, remain in effect except that the ~~phased in~~ compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7.

The Responsible Entity shall not be required to include in its cyber security plan(s) elements related to Sections 2 and 3 of Attachment 1 until the effective date of CIP-003-7. Upon the effective date of CIP-003-7, the Responsible Entity's cyber security plan(s) must include the elements required by Sections 2 and 3 of Attachment 1 and the Responsible Entity must implement the controls included ~~therein~~in its plan to meet the objectives of Sections 2 and 3.

Effective Date

The effective date for the proposed Reliability Standard ~~and NERC Glossary term~~ is provided below:

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7 ~~and the NERC Glossary term *Low Impact External Routable Communication* (LERC)~~ shall become effective on the later of September 1, 2018 or the first day of the first calendar quarter that is ~~nine (9~~twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-7 ~~and the NERC Glossary term *Low Impact External Routable Communication* (LERC)~~ shall become effective on the first day of the first calendar quarter that is ~~nine (9~~twelve (12) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Planned or Unplanned Changes

Planned or Unplanned Changes Resulting in a Higher Categorization – This implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-5 titled Planned or Unplanned Changes Resulting in a Higher Categorization.[1]

Unplanned Changes Resulting in Low Impact Categorization – This implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-6 titled Unplanned Changes Resulting in Low Impact Categorization. That section provides:

> For unplanned changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

Retirement Date

Reliability Standard CIP-003-6

Reliability Standard CIP-003-6 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-7 in the particular jurisdiction in which the revised standard is becoming effective.

Current NERC Glossary of Terms of LERC and LEAP

The current definition of LERC and the term LEAP shall be retired from the NERC Glossary of Terms immediately prior to the effective date of ~~the revised LERC term~~CIP-003-7 in the particular jurisdiction in which the definition is becoming effective.

[1] Due to the length of that section, it is not reproduced herein.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Modifications to address the FERC directive regarding the Definition of Low Impact External Routable Connectivity

Do not use this form for submitting comments. Use the electronic form to submit comments on the **Modifications to address the Federal Energy Regulatory Commission directive regarding the Definition of Low Impact External Routable Connectivity**. The electronic form must be submitted by **8 p.m. Eastern, Monday, December 5, 2016.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer Al McMeekin (via email) or at (404) 446-9675.

Background Information

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, Revised Critical Infrastructure Protection Reliability Standards, approving seven CIP Reliability Standards and new or modified definitions. In Order No. 822, the Commission also directed NERC to make certain modifications to those standards and definitions. On March 9, 2016, the NERC Standards Committee authorized the Standards Authorization Request (SAR) to be posted for a 30-day informal comment period from March 23 – April 21, 2016. Based on the comments received, the 2016-02 Modifications to CIP Standards Drafting Team (SDT) made minor revisions to the SAR which was posted for an additional 30-day informal comment period June 1-30, 2016.

In Order 822, the Commission stated:

> "73. Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6."

SDT Approach

In this revision, the terms *Low Impact External Routable Connectivity* (LERC) and *Low Impact BES Cyber System Electronic Access Point* (LEAP) have been deleted and the requirements for electronic access controls for asset(s) containing low impact BES Cyber Systems simplified so that it is an attribute of a BES asset. The SDT modified the requirements to permit only inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a

Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls, unless that communication meets the exclusion language. The defined term LEAP is no longer necessary because the SDT changed the requirement from requiring a LEAP to requiring electronic access controls. Additionally, since the SDT is removing the term LERC, the exclusion language that was previously in the definition of LERC was integrated into the Attachment 1, Section 3.1 requirement.

Because the proposed modifications to Reliability Standard CIP-003-7 eliminate the need for the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP), NERC is requesting these terms be retired in the associated implementation plan.

Additionally, the SDT:

- revised the associated Lower, Moderate, and High VSLs for Requirement R2 to complement the requirement revisions;
- corrected a mistake in the Severe VSL for Requirement R2;
- made non-substantive changes to the Moderate and High VSLs for Requirement R2 to align with the order of the requirement;
- removed repetitive text from Requirement R1, Part 1.2.3 to make it consistent with Parts 1.2.1 and 1.2.2;
- updated the Guidelines and Technical Basis section of the standard to reflect the revisions made to the Attachments;
- made non-substantive errata changes throughout the standard such as replacing “ES-ISAC” with “E-ISAC”; and
- revised the Implementation Plan to reflect revisions to the draft standard and to provide additional clarity.

The SDT requests feedback on the proposed approach to addressing the FERC directive.

Questions

1. Definition: The SDT is proposing the retirement of the terms Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP). The SDT incorporated the LERC concepts into the Requirement R2 language and removed the LERC reference from Requirement R1, Part 1.2.3 and the LEAP references from Attachment 1, Sections 2 and 3.1. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

2. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 3 to require each Responsible Entity to implement electronic access controls for each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002 that permit only necessary inbound and outbound electronic access as determined by the Responsible Entity. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

3. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 2 Physical Security Controls to reflect the retirement of LEAP. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

4. Attachment 2: The SDT revised the complementary language of CIP-003-6, Attachment 2, Sections 2 and 3 to make the evidential language of the measure consistent with the revised requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides example diagrams that illustrate various electronic access controls at a conceptual level. Do you agree with the revisied content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

   Yes:

   No:

   Comments:

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) date for the revisions made to CIP-003, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer, please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

   Yes:

   No:

   Comments:

7. If you have additional comments on the proposed revisions to address the FERC directive regarding the LERC definition that you have not provided in response to the questions above, please provide them here.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 – Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factor (VRF) and violation severity levels (VSLs) for Requirement R2 in proposed NERC Reliability Standard CIP-003-7 - Cyber Security — Security Management Controls. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-003-7, Requirement R2	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Lower was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements for low impact BES Cyber Systems. The purpose of plans is for entities to develop an approach involving multiple procedures to address a broad subject matter. Using a plan, Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems.
FERC VRF G1 Discussion Guideline 1 - Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2 - Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement a documented cyber security plan that contains certain sections specified in Attachment 1. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security plan, the VRF is reflective of the plan as a whole. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain low impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3 - Consistency among Reliability Standards	This requirement maps from CIP-003-5, Requirement R1, which has an approved VRF of Medium but applies to Cyber Assets with an inherently lower risk; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Failure to properly implement the cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state

VRF Justifications for CIP-003-7, Requirement R2	
Proposed VRF	**Lower**
Guideline 4 - Consistency with NERC Definitions of VRFs	or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion Guideline 5 - Treatment of Requirements that Co-mingle More than One Obligation	The cyber security plan requirement encompasses a number of subject matter areas for low impact BES Cyber Systems. The VRF is identified at the risk level represented by all of the plan areas in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.

VSLs for CIP-003-7, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2)	low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its	low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)	

	assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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.		

VSL Justifications for CIP-003-7, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved Requirement R2, CIP-003-6. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-003-7, Requirement R2	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security plan(s) but fails to address one or more of the required sections of Attachment 1. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The action of the requirement is to implement documented cyber security plan(s). Documentation of the plan(s) is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the plan in this case; as such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity implemented all the required elements of the plan. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 – Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factor~~s~~ (VRF~~s~~) and violation severity levels (VSLs) for ~~each r~~Requirement R2 in proposed NERC Reliability Standard CIP-003-7 - Cyber Security — Security Management Controls~~Project 2016-02, Modifications to CIP Standards~~. ~~Each requirement is assigned a VRF and a VSL.~~ These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-003-7, Requirement R2	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Lower was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements for low impact BES Cyber Systems. The purpose of plans is for entities to develop an approach involving multiple procedures to address a broad subject matter. Using a plan, Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems.
FERC VRF G1 Discussion Guideline 1 - Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2 - Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement a documented cyber security plan that contains certain sections specified in Attachment 1. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security plan, the VRF is reflective of the plan as a whole. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain low impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3 - Consistency among Reliability Standards	This requirement maps from CIP-003-5, Requirement R1, which has an approved VRF of Medium but applies to Cyber Assets with an inherently lower risk; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Failure to properly implement the cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state

VRF Justifications for CIP-003-7, Requirement R2	
Proposed VRF	**Lower**
Guideline 4 - Consistency with NERC Definitions of VRFs	or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion Guideline 5 - Treatment of Requirements that Co-mingle More than One Obligation	The cyber security plan requirement encompasses a number of subject matter areas for low impact BES Cyber Systems. The VRF is identified at the risk level represented by all of the plan areas in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.

VSLs for CIP-003-7, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing	The Responsible Entity failed to document ~~or~~and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2)	low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its	low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)	

	assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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. ~~OR~~ ~~The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to~~	~~OR~~ ~~The Responsible Entity documented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to implement the electronic access controls to low impact BES Cyber Systems according to Requirement R2, Attachment 1, Section 3. (R2)~~ ~~OR~~ ~~The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)~~	

	~~Requirement R2, Attachment 1, Section 2. (R2)~~ ~~OR~~ ~~The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)~~		

VSL Justifications for CIP-003-7, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved Requirement R2, CIP-003-6. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-003-7, Requirement R2	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security plan(s) but fails to address one or more of the required sections of Attachment 1. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The action of the requirement is to implement documented cyber security plan(s). Documentation of the plan(s) is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the plan in this case; as such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity implemented all the required elements of the plan. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

Consideration of Issues and Directives

Project 2016-02 Modifications to CIP Standards

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.	FERC Order 822, Paragraph 73; issued January 21, 2016	The Project 2016-02 Standard Drafting Team (SDT) resolved the ambiguity identified by the Commission surrounding the term "direct" within the definition of Low Impact External Routable Connectivity (LERC) by retiring the term and incorporating the LERC concepts within the requirement language. Retiring the LERC definition removes the dependency between the electronic access controls that may be in place and having those controls determine whether LERC exists or not. The SDT determined that indirect access, regardless of what kind of security break is in place causing it to be indirect, is another form of electronic access control that is intended to meet the same security objective. The SDT determined that the requirements should address the electronic access controls rather than having some controls implied through the definition. In changing the approach, the SDT avoids overemphasis on identifying LERC and focuses emphasis on the security objective in the requirements. Therefore, for those assets containing low impact BES Cyber Systems as identified in CIP-002, the SDT changed the language in Attachment 1, Section 3.1 from requiring a Low Impact Electronic Access Point (LEAP) to requiring that electronic access controls be implemented to meet the security objective of

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		permitting "only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s); ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and, iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)." Additionally, the SDT updated and incorporated the exclusion language from the approved LERC definition into the requirement language and expanded the Guidelines and Technical Basis with numerous examples of electronic access control concepts that accomplish the defined security objective. Given the proposed retirement of LERC and the proposed modifications in Reliability CIP-003-7, there is no longer a need for the NERC Glossary term Low Impact BES Cyber System Electronic Access Point (LEAP). Consequently, the SDT proposed the term's retirement.

Consideration of Issues and Directives

Project 2016-02 Modifications to CIP Standards

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.	FERC Order 822, Paragraph 73; issued January 21, 2016	The Project 2016-02 Standard Drafting Team (SDT) ~~revised~~resolved the ambiguity identified by the Commission surrounding the term "direct" within the definition of ~~the term~~ Low Impact External Routable Connectivity ~~to resolve the ambiguity surrounding the term "direct" identified by the Commission. In doing so,~~(LERC) by retiring the term and incorporating the ~~SDT changed~~LERC concepts within the ~~term to Low Impact External Routable *Communication* (LERC) and simplified~~requirement language. Retiring the ~~definition so that LERC is an attribute of an asset containing low impact BES Cyber Systems. As revised, LERC exists where there is routable protocol communication that crosses the asset boundary without regard to whether 'direct' or 'indirect' access may occur. The revised~~ LERC definition removes the dependency between the electronic access controls that may be in place and having those controls determine whether LERC exists or not. The SDT determined that indirect access, regardless of what kind of ~~'~~security break~~'~~ is in place causing it to be indirect, is another form of electronic access control that is intended to meet the same security objective. The SDT determined that the requirements should address the electronic access controls rather than having some controls

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		implied through the definition. In changing the approach, the SDT avoids overemphasis on identifying LERC and focuses emphasis on the security objective in the requirements. Therefore, for those assets containing low impact BES Cyber Systems ~~that have LERC~~as identified in CIP-002, the SDT changed the language in Attachment 1, Section 3.1 from requiring a Low Impact Electronic Access Point (LEAP) to requiring that electronic access controls be implemented to meet the security objective of permitting "only necessary inbound and outbound electronic access ~~to~~as determined by the Responsible Entity for any communications that are: i. between a low impact BES Cyber ~~Systems."~~ System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s); ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and, iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)." Additionally, the SDT updated and incorporated the exclusion language from the approved LERC definition into the requirement language and expanded the Guidelines and Technical Basis with numerous examples of electronic access

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		control concepts that accomplish ~~this~~the defined security objective. Given the ~~modified definition~~proposed retirement of LERC and the proposed modifications in Reliability CIP-003-7, there is no longer a need for the NERC Glossary term Low Impact BES Cyber System Electronic Access Point (LEAP). Consequently, the SDT proposed the term's retirement.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Reminder

Project 2016-02 Modifications to CIP Standards

Additional Ballots and Non-binding Poll Open through December 5, 2016

Now Available

The following ballots are open through **8 p.m. Eastern, Monday, December 5, 2016**:

1. **Addtional ballot for CIP-003-7 - Cyber Security – Security Management Controls**
2. **Additional ballot for CIP-003-7 Implementation Plan**
3. **Non-binding poll of the associated Violation Risk Factors and Violation Severity Levels**

Balloting

Members of the ballot pools associated with this project may log in and submit their vote for the standard and its implementation plan, and the non-binding poll by clicking here. If you experience any difficulties in using the electronic form, contact Wendy Muller.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Al McMeekin at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Period Open through December 5, 2016

Now Available

A 45-day formal comment period **CIP-003-7 - Cyber Security – Security Management Controls** and the **CIP-003-7 implementation plan** is open through **8 p.m. Eastern, Monday, December 5, 2016.**

Commenting

Use the electronic form to submit comments. If you experience any difficulties using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

Next Steps

Additional ballots for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **November 23 – December 5, 2016**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Al McMeekin (via email) or at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/68)
Ballot Name: 2016-02 Modifications to CIP Standards CIP-003-7 AB 2 ST
Voting Start Date: 11/23/2016 12:01:00 AM
Voting End Date: 12/5/2016 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 259
Total Ballot Pool: 339
Quorum: 76.4
Weighted Segment Value: 85.56

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	46	0.767	14	0.233	0	5	21
Segment: 2	7	0.1	1	0.1	0	0	0	2	4
Segment: 3	75	1	49	0.845	9	0.155	0	2	15
Segment: 4	26	1	17	0.944	1	0.056	0	2	6
Segment: 5	80	1	42	0.792	11	0.208	0	3	24
Segment: 6	48	1	31	0.756	10	0.244	0	1	6
Segment: 7	3	0	0	0	0	0	0	1	2
Segment: 8	3	0.2	2	0.2	0	0	0	0	1
Segment: 9	2	0.2	2	0.2	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.7	7	0.7	0	0	0	1	1
Totals:	339	6.2	197	5.304	45	0.896	0	17	80

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Negative	Comments Submitted
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	American Transmission Company, LLC	Andrew Pusztai		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Third-Party Comments
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		None	N/A
1	Bonneville Power Administration	Donald Watkins		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	Third-Party Comments
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Shawna Speer		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Negative	Comments Submitted
1	Duke Energy	Doug Hils		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass	Matt Stryker	Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Abstain	N/A
1	JEA	Ted Hobson	Joe McClung	None	N/A
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		None	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Third-Party Comments
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Third-Party Comments
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Abstain	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Abstain	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		None	N/A
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		Abstain	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		None	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		None	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Third-Party Comments
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Negative	Comments Submitted
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		None	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Affirmative	N/A
3	Gainesville Regional Utilities	Ken Simmons		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Affirmative	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		None	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Abstain	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		Affirmative	N/A
4	Austin Energy	Tina Garvey		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Affirmative	N/A
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		None	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Third-Party Comments
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Abstain	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Michael Ward		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		None	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		None	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Affirmative	N/A
5	JEA	John Babik		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Kissimmee Utility Authority	Mike Blough		None	N/A
5	Lakeland Electric	Jim Howard		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		None	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Wayne Sipperly		Negative	Comments Submitted
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		None	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Third-Party Comments
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Abstain	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer		Abstain	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		None	N/A
5	Seattle City Light	Mike Haynes		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		None	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		None	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Salt River Project	Chris Janick		Affirmative	N/A
6	Santee Cooper	Michael Brown		None	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Negative	Third-Party Comments
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Elizabeth Davis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	Westar Energy	Megan Wagner		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		Abstain	N/A
7	Luminant Mining Company LLC	Stewart Rake		None	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		None	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Abstain	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 339 of 339 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/68)
Ballot Name: 2016-02 Modifications to CIP Standards CIP-003-7 Implementation Plan AB 2 OT
Voting Start Date: 11/23/2016 12:01:00 AM
Voting End Date: 12/5/2016 8:00:00 PM
Ballot Type: OT
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 259
Total Ballot Pool: 338
Quorum: 76.63
Weighted Segment Value: 75.54

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	43	0.694	19	0.306	0	3	20
Segment: 2	7	0.1	1	0.1	0	0	0	2	4
Segment: 3	75	1	40	0.702	17	0.298	0	3	15
Segment: 4	26	1	13	0.684	6	0.316	0	1	6
Segment: 5	80	1	36	0.679	17	0.321	0	3	24
Segment: 6	48	1	28	0.7	12	0.3	0	2	6
Segment: 7	3	0	0	0	0	0	0	1	2
Segment: 8	3	0.2	2	0.2	0	0	0	0	1
Segment: 9	2	0.2	2	0.2	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.8	8	0.8	0	0	0	0	1
Totals:	338	6.3	173	4.759	71	1.541	0	15	79

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Negative	Comments Submitted
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	American Transmission Company, LLC	Andrew Pusztai		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Third-Party Comments
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Bonneville Power Administration	Donald Watkins		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	Third-Party Comments
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Shawna Speer		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Negative	Comments Submitted
1	Duke Energy	Doug Hils		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		None	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Jason Snodgrass	Matt Stryker	Negative	Comments Submitted
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Abstain	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	None	N/A
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		None	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		None	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Third-Party Comments
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Negative	Comments Submitted
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Third-Party Comments
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Abstain	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Howell Scott		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Negative	Third-Party Comments
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		None	N/A
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		Abstain	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		None	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		None	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Third-Party Comments
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Negative	Comments Submitted
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		None	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Affirmative	N/A
3	Gainesville Regional Utilities	Ken Simmons		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Third-Party Comments
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Abstain	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Negative	Comments Submitted
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Santee Cooper	James Poston		None	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		None	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Bo Jones		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Michael Ibold		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Abstain	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		Negative	Comments Submitted
4	Austin Energy	Tina Garvey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City of Clewiston	Lynne Mila	Chris Gowder	Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Affirmative	N/A
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Negative	Third-Party Comments
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Negative	Comments Submitted
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Third-Party Comments
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seminole Electric Cooperative, Inc.	Michael Ward		None	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Comments Submitted
5	AEP	Thomas Foltz		None	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Negative	Third-Party Comments
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Third-Party Comments
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		None	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		None	N/A
5	Lakeland Electric	Jim Howard		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		None	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Abstain	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Wayne Sipperly		Negative	Comments Submitted
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		None	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Third-Party Comments
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer		Abstain	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		None	N/A
5	Seattle City Light	Mike Haynes		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Negative	Third-Party Comments
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		None	N/A
5	WEC Energy Group, Inc.	Linda Horn		Negative	Comments Submitted
5	Westar Energy	Laura Cox		Negative	Third-Party Comments
5	Xcel Energy, Inc.	David Lemmons		Negative	Third-Party Comments
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Third-Party Comments
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Third-Party Comments
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		None	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Salt River Project	Chris Janick		Affirmative	N/A
6	Santee Cooper	Michael Brown		None	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Affirmative	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Negative	Third-Party Comments
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Talen Energy Marketing, LLC	Elizabeth Davis		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	Third-Party Comments
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	Westar Energy	Megan Wagner		Negative	Third-Party Comments
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Exxon Mobil	Jay Barnett		Abstain	N/A
7	Luminant Mining Company LLC	Stewart Rake		None	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		None	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 338 of 338 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/68)
Ballot Name: 2016-02 Modifications to CIP Standards CIP-003-7 Non-binding Poll AB 2 NB
Voting Start Date: 11/23/2016 12:01:00 AM
Voting End Date: 12/5/2016 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 240
Total Ballot Pool: 320
Quorum: 75
Weighted Segment Value: 82.47

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	36	0.766	11	0.234	15	18
Segment: 2	7	0.1	1	0.1	0	0	2	4
Segment: 3	75	1	43	0.878	6	0.122	10	16
Segment: 4	23	1	13	0.929	1	0.071	4	5
Segment: 5	73	1	30	0.769	9	0.231	9	25
Segment: 6	45	1	26	0.788	7	0.212	5	7
Segment: 7	3	0	0	0	0	0	1	2
Segment: 8	3	0.2	2	0.2	0	0	0	1
Segment: 9	2	0.2	2	0.2	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	9	0.7	7	0.7	0	0	0	2
Totals:	320	6.2	160	5.329	34	0.871	46	80

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	Abstain	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Bonneville Power Administration	Donald Watkins		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Abstain	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	Comments Submitted
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Shawna Speer		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Abstain	N/A
1	Duke Energy	Doug Hils		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		None	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass	Matt Stryker	Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	None	N/A
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Danny Pudenz		Abstain	N/A
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		None	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		None	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Abstain	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Affirmative	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Abstain	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Abstain	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Abstain	N/A
2	California ISO	Richard Vine		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry Bllke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		None	N/A
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		Abstain	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Abstain	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		None	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		None	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City of Leesburg	Chris Adkins	Chris Gowder	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Negative	Comments Submitted
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Abstain	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		None	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Affirmative	N/A
3	Gainesville Regional Utilities	Ken Simmons		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Affirmative	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Abstain	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		None	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		None	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Abstain	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		Affirmative	N/A
4	Austin Energy	Tina Garvey		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Affirmative	N/A
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Abstain	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	LaGen	Richard Comeaux		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Abstain	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Michael Ward		None	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		None	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Abstain	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		None	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Affirmative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		None	N/A
5	Lakeland Electric	Jim Howard		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		None	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		None	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Abstain	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	Nebraska Public Power District	Don Schmit		Abstain	N/A
5	New York Power Authority	Wayne Sipperly		Negative	Comments Submitted
5	NextEra Energy	Allen Schriver		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Comments Submitted
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Abstain	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer		Abstain	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		None	N/A
5	Seattle City Light	Mike Haynes		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	William D. Shultz		Negative	Comments Submitted
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		None	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Abstain	N/A
5	U.S. Bureau of Reclamation	Wendy Center		None	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Comments Submitted
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		None	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Comments Submitted
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Abstain	N/A
6	Salt River Project	Chris Janick		Affirmative	N/A
6	Santee Cooper	Michael Brown		None	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Affirmative	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Negative	Comments Submitted
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Elizabeth Davis		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Westar Energy	Megan Wagner		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		Abstain	N/A
7	Luminant Mining Company LLC	Stewart Rake		None	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		None	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		None	N/A

Previous 1 Next

Showing 1 to 320 of 320 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Period Open through December 5, 2016

Now Available

A 45-day formal comment period **CIP-003-7 - Cyber Security – Security Management Controls** and the **CIP-003-7 implementation plan** is open through **8 p.m. Eastern, Monday, December 5, 2016.**

Commenting

Use the electronic form to submit comments. If you experience any difficulties using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

Next Steps

Additional ballots for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **November 23 – December 5, 2016**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Al McMeekin (via email) or at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | CIP-003-7 and Implementation Plan
Comment Period Start Date:	10/21/2016
Comment Period End Date:	12/5/2016
Associated Ballots:	2016-02 Modifications to CIP Standards CIP-003-7 AB 2 ST 2016-02 Modifications to CIP Standards CIP-003-7 Implementation Plan AB 2 OT 2016-02 Modifications to CIP Standards CIP-003-7 Non-binding Poll AB 2 NB

There were 61 sets of responses, including comments from approximately 58 different people from approximately 54 companies representing 9 of the Industry Segments as shown in the table on the following pages.

Questions

1. Definition: The SDT is proposing the retirement of the terms Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP). The SDT incorporated the LERC concepts into the Requirement R2 language and removed the LERC reference from Requirement R1, Part 1.2.3 and the LEAP references from Attachment 1, Sections 2 and 3.1. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

2. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 3 to require each Responsible Entity to implement electronic access controls for each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002 that permit only necessary inbound and outbound electronic access as determined by the Responsible Entity. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

3. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 2 Physical Security Controls to reflect the retirement of LEAP. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

4. Attachment 2: The SDT revised the complementary language of CIP-003-6, Attachment 2, Sections 2 and 3 to make the evidential language of the measure consistent with the revised requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides example diagrams that illustrate various electronic access controls at a conceptual level. Do you agree with the revisied content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) date for the revisions made to CIP-003, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer, please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

7. If you have additional comments on the proposed revisions to address the FERC directive regarding the LERC definition that you have not provided in response to the questions above, please provide them here.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Chris Gowder	Chris Gowder		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utility Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steve Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Mark Brown	City of Winter Park	4	FRCC
					Chris Adkins	City of Leesburg	3	FRCC

					Ginny Beigel	City of Vero Beach	9	FRCC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
ACES Power Marketing	Colleen Campbell	6	NA - Not Applicable	ACES Standards Collaborators	Shari Heino	Brazos Electric Power Cooperative, Inc.	1,5	Texas RE
					John Shaver	Arizona Electric Power Cooperative, Inc.	1	WECC
					Mike Brytowski	Great River Energy	1,3,5,6	MRO
					Ryan Strom	Buckeye Power, Inc	4	RF
					Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	RF
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Watson	Old Dominion Electric Cooperative	3,4	SERC
					Wes Moody	East Kentucky Power Cooperative	1,3	SERC
					Paul Mehlhaff	Sunflower Electric Power Corporation	1,5	SPP RE
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC

					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,10	NPCC	RSC no Dominion	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					David Ramkalawan	Ontario Power Generation	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Kelly Silver	Con Edison	3	NPCC

					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Chuck Lawrence	American Transmission Company	1	MRO
					Chuck Wicklund	Otter Tail Power Company	1,5	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Shannon Weaver	Midcontinent Independent System Operator	2	MRO
					Brad Parret	Minnesota Power	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO

					Tony Eddleman	Nebraska Public Power District	1,3,5	MRO
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Louis Guidry	Cleco Power	1,3,5,6	SPP RE
					Steve Keller	Southwest Power Pool Inc	2	SPP RE
					Robert Hirchak	Cleco Power	1,3,5,6	SPP RE
Public Service Enterprise Group	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF

1. Definition: The SDT is proposing the retirement of the terms Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP). The SDT incorporated the LERC concepts into the Requirement R2 language and removed the LERC reference from Requirement R1, Part 1.2.3 and the LEAP references from Attachment 1, Sections 2 and 3.1. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST appreciates the SDT's efforts to address Order 822's directive to add clarity to the definition of LERC. However, we believe that simply retiring the term will not adequately resolve the fundamental question of when, and under what conditions, electronic access controls (draft CIP-003-7 Attachment 1 Section 3) must be applied in order to protect low impact BES Cyber Systems (see N&ST comments on "Guidelines and Technical Basis," following). Accordingly, N&ST suggests taking advantage of the existing, industry, NERC and FERC approved of "External Routable Connectivity" and modifying it for low impact as follows: LERC = "The ability to access a low impact BES Cyber System from a Cyber Asset that is outside of the BES asset in which it is contained via a bi-directional routable protocol connection." The exception for point-to-point connections between IEDs for time-sensitive control and protection functions can be retained from the original LERC definition. N&ST wishes to point out this proposed definition does not in any way introduce the concept of an Electronic Security Perimeter to low impact environments, which is something that FERC has indicated it is presently not inclined to require (Order 822, paragraph 75).

N&ST agrees with the proposed retirement of the term, "LEAP."

Likes 0	
Dislikes 0	
Response	

David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	No
Document Name	
Comment	

CIP-003-7 draft currently states that the Responsible Entity (RE) shall implement electronic access controls, but it does not clearly state in CIP-003 Attachment 1 Section 3.1 that electronic access controls are only required IF all three criteria is present. Please modify the CIP-003 Attachment 1 Section 3.1 to clearly state that. In addition, please consider adding a statement that if the criteria is not applicable, i.e., if there is not "a routable protocol", the RE is not required to establish electronic access controls.

Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST appreciates the SDT's efforts to address Order 822's directive to add clarity to the definition of LERC. However, we believe that simply retiring the term will not adequately resolve the fundamental question of when, and under what conditions, electronic access controls (draft CIP-003-7 Attachment 1 Section 3) must be applied in order to protect low impact BES Cyber Systems (see N&ST comments on "Guidelines and Technical Basis," following). Accordingly, N&ST suggests taking advantage of the existing, industry, NERC and FERC approved of "External Routable Connectivity" and modifying it for low impact as follows: LERC = "The ability to access a low impact BES Cyber System from a Cyber Asset that is outside of the BES asset in which it is contained via a bi-directional routable protocol connection." The exception for point-to-point connections between IEDs for time-sensitive control and protection functions can be retained from the original LERC definition. N&ST wishes to point out this proposed definition does not in any way introduce the concept of an Electronic Security Perimeter to low impact environments, which is something that FERC has indicated it is presently not inclined to require (Order 822, paragraph 75).

N&ST agrees with the proposed retirement of the term, "LEAP."

Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

The description of the current draft states:

"The SDT simplified Section 3 of Attachment 1 to require the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the exclusion language (previously in the definition of LERC) contained in (iii) which reads: "not used for time -sensitive protection or control GOOSE)"."

This unnecessarily includes all communications traffic which may not even be destined for a BES cyber system at that site. As a matter of normal operation our internal communications network switches traffic through site which are not the final destination for the traffic. This new definition would bring all of that traffic unnecessarily into scope. Even if the requirements to adhere to the applicable standard are low, Idaho Power will be spend unnecessary dollars on keep track of and report on this.

The definition should be modified to only include traffic destined for a local BES cyber system. An additional exception stating "excluding traffic not destined for a local BES cyber system." The SDT does not seem to understand that not all traffic crossing an asset boundary is destined for that asset, some traffic may continue on from the asset to other assets. Traffic destined for other assets should not be controlled and specifically permitted at every stop along the way. It should be controlled at the communications ingress and egress points only.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5

Answer	No
Document Name	

Comment

While the revisions to CIP-003 obviate the need for the problematice LERC and LEAP definitions, they retain some of the ambiguity regarding physical versus logical characteristics. Suggested revision:

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

i. between a low impact BES Cyber System(s) and an external network(s) or a Cyber Asset(s) residing outside of a network to which low impact BES Cyber System(s) are connected;

ii. using a routable protocol when entering or leaving the network on which the low impact BES Cyber System(s) reside; and,

iii. not used for time IEC TR protectio
61850 -90-5 R-GOOSE).”

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy requests further clarification from the drafting team regarding the removal of the term “bi directional”from Section 3 in Attachment 1. Is it the drafting team’s interpretation that the term “bi directional” was redundant, and thus not necessary in the language? The term “bi directional” is not included in the definition of “Routable Protocol,” and removing the term in this instance promotes ambiguity, and could impact applicability of the standard.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	

1) The SDT's approach to retire the definitions of LERC and LEAP by implementing low impact electronic access controls is one way to address the directive in FERC Order No. 822, which focused on the ambiguity of the word "direct." However, this approach creates unintended consequences for compliance. In particular, the proposed revisions implicitly require low impact entities to have an identified list of low impact assets, which is specifically excluded in CIP-002.

2) The SDT's proposed approach will create difficulty for both industry to demonstrate compliance and for auditors to determine reasonable assurance.

3) We suggest the SDT consider another method to address the FERC directive that still preserves the low impact requirements and the explicit exclusion from being required to have an inventory list of low impact assets.

4) One possible approach is for low impact entities to have a documented process that applies electronic access controls to low impact assets.

a. Auditors could verify that the entity has developed the documented process, and the entity could demonstrate compliance by providing the document as evidence.

b. This approach also preserves the disparate treatment of low and medium impact assets, by assigning different levels of requirements that are commensurate with the risks they pose to the Bulk Electric System.

Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	

As the SDT doesn't appear to have made any changes to R2, we are confused as to how LERC concepts were incorporated via only the removal of the defined terms.

The retirement of the terms Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) provides less clarity in the information addressing electronic access controls in section R1 - 1.2.3.

Also, R1.2 mentions assets identified in CIP-002 and low impact BES Cyber Systems. However, it is unclear whether the parts listed below (Parts 1.2.1 - 1.2.4) are creating requirements associated with CIP-002 or CIP-003-7.

Changing “specified” to “identified” in the following: “and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.” will make the electronic access device more clearly defined by the entity.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
LADWP technical standards and policies for equipment and infrastructure inherently provide the security attributes required by the proposed changes to CIP-003-7.	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA supports the retirement of LERC and LEAP and the removal of references in Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
City Light has no comments for Q1	

Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the removal of the terms LERC and LEAP and appreciates the SDT for simplifying the requirement language. After reviewing where the language was replaced, SRP agrees with the verbiage used to substitute the terms. Additionally, SRP appreciates the removal of the use of asset boundary from the language. The requirements are much clearer than before.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
The concepts that replaced the Defined Terms are an improvement from the previous definitions for LERC and LEAP. The new concept puts emphasis in protecting BES Cyber Assets, but lacks clarity on how compliance with the Standard will be achieved.	

Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
The concepts that replaced the Defined Terms are an improvement from the previous definitions for LERC and LEAP. The new concept puts emphasis in protecting BES Cyber Assets, but lacks clarity on how compliance with the Standard will be achieved.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC	
Answer	Yes
Document Name	
Comment	
Reclamation commends the SDT on this effort to simplify the standard.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Blair Mukanik - Manitoba Hydro - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Yuguang Xiao - Manitoba Hydro - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Alexander Vedvik - Public Service Commission of Wisconsin - 9	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 1	Hydro One Networks, Inc., 3, Malozewski Paul
Dislikes 0	
Response	
Paul Malozewski - Hydro One Networks, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael DeLoach - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rich Hydzik - Rich Hydzik On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Rich Hydzik	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Michael Mertz - PNM Resources - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE appreciates the SDT's continued efforts to develop a workable definition of Low Impact External Routable Connectivity (LERC) that addresses FERC's directive in Order No. 822. As FERC's directive made clear, the focus of this project should be on developing a workable modification to the LERC definition consistent with "the commentary in the Guidelines and Technical Basis section of CIP-003-6." In fulfilling this mandate, the SDT has elected to retire the LERC definition and instead incorporate elements of the LERC and Low-Impact BES Cyber System Electronic Access Point (LEAP) concepts into a new requirement focused on electronic access controls. While the SDT's approach appears to also meet the terms of the FERC directive, Texas RE remains concerned that introducing such new concepts may lead to confusion. Given this fact, Texas RE continues to believe that the better approach is to draw from facility Electronic Access Point concepts already set forth in CIP-005. As such, Texas RE proposes the following revision to Attachment 2, Section 3.1 in lieu of the SDT's current approach: *Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default."*. With this change, Texas RE's proposed Section 3.1 would read as follows:

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber

System(s) identified pursuant to CIP -002, the Responsible Entity shall implement

electronic access controls to:

3.1 *Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default* for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and,

iii. not used for time communications using protocol IEC TR 61850 -90-5 R-GOOSE).

3.2 Authenticate all Dial ity.

Texas RE believes that such an approach would make the CIP Standards more consistent with one another while avoiding introducing new and untested concepts in a project designed to have a limited scope.

Texas RE acknowledges that FERC did not direct NERC to utilize the concept of Electronic Security Perimeters for low impact systems and to leverage existing definitions for EAP and ERC. However, given the approach taken by the SDT in response to FERC's narrow directive, Texas RE believes that the SDT may wish to consider extending the familiar concepts in the existing ERC definition to the LERC environment at this juncture as part of the developing a new electronic access control requirements.

Likes 0	
Dislikes 0	

Response

Tim Kucey - PSEG - PSEG Fossil LLC - 5

Answer	
Document Name	

Comment

adopt PSEG comments

Likes 0	
Dislikes 0	

Response

2. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 3 to require each Responsible Entity to implement electronic access controls for each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002 that permit only necessary inbound and outbound electronic access as determined by the Responsible Entity. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

We suggest the drafting team re-evaluate the electronic access control is required. We feel that the electronic access control should be applied to each of the low impact BES Cyber System(s) in the identified asset containing low impact BES Cyber Assets instead of the asset that contains the low impact Cyber Systems.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators

Answer	No
Document Name	

Comment

1) This requirement suggests that Responsible Entities must identify or otherwise list their low impact Cyber Assets similar in nature to a medium-impact requirement; otherwise how will compliance be evaluated? This approach contradicts CIP-002, which states an inventory list of low impact BES Cyber Systems (or Cyber Assets) is not required.

2) Responsible Entities are *only* required to implement electronic access controls to assets containing low impact BES Cyber Systems with *necessary* inbound and outbound electronic access. There does not appear to be much clarity around the criteria for access “necessity” and therefore the benchmark for the requirement of implementing electronic access controls is unclear and unmeasurable. How will compliance with this be evaluated?

3) Consider requiring a documented methodology for implementing electronic access controls for each asset containing low impact BES Cyber Systems.

a. This alleviates any implied requirement for maintaining an inventory list of low impact assets, and would allow the Responsible Entity to incorporate use of exclusion criteria to those communications it deems applicable.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
SMUD/BANC is not supportive of the proposed changes to Attachment 1-Section 3. It is confusing what is the necessary treatment for cyber assets included in a “Facility” but not a BES Cyber System. In addition the definition of terms regarding “asset”, “routable communication”, “any communication”, and “electronic access” as included in attachment 1 and the supplemental information is necessary for clarification and applicability.	
Likes 0	
Dislikes 0	
Response	
Michael DeLoach - AEP - 3	
Answer	No
Document Name	
Comment	
Question is not written consistant with the proposed Section 2 language. The electronic access controls are to be applied to the external (to the asset) routable communications from/to low impact BES Cyber Systems not all routable communications to the asset. Comments: The wording under Section 3 item ii brings into scope every routable connection that enters or leaves an asset containing low impact BES Cyber System. This is an overly broad classification and reaches beyond the regulation of equipment involved in the operation of the BES. There can be multiple routable conections into and out of an asset containing low impact BES Cyber Ssytems that provide no connection to low impact BES Cyber Assets. Item ii should be removed from Section 3.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy recommends the following language change to Attachment 1, Section 3.1 i:	

“between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset, as determined by the Responsible Entity, containing low impact BES Cyber System(s);”

We feel that the addition of “as determined by the Responsible Entity” is necessary in that it reduces ambiguity, and promotes consistency with other aspects of this section.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5

Answer	No
Document Name	

Comment

Please see above comments regarding physical and logical characteristics.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

MMWEC is voting to approve with the following comment:

MMWEC recommends changing the proposed CIP-003-7 Attachment 1, Section 3.1(ii) to the following:

"ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber Systems(s) or using a routable protocol when the BES Cyber Asset is addressable using a routable protocol from outside the asset; and,”

Rationale

As currently written the criteria in Attachment 1, Section 3.1 for requiring electronic access controls would exempt communication to a BES Cyber Asset that uses an IP to serial protocol converter if that converter is located outside of the asset and only serial communications enter the asset. This would be the case even if the protocol converter faces the public Internet.

The GTB (p. 33) states that entities can “identify an ‘electronic boundary’ associated with the asset.” Thus, an entity could designate the electronic boundary to be between the BES Cyber Asset and the protocol converter in order to assert that there is no routable communications crossing the

electronic boundary. Although compliant, this would not be secure, since the BES Cyber Asset would be addressable from a Cyber Asset located outside the asset.

The recommended change to Section 3.1(ii) would reduce the risk of BES Cyber Assets that are connected to the Internet by a protocol converter from being identified by tools such as Shodan.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

This section needs to be modified to be congruent with a LERC definition which is allows for the exception of traffic not destined for a local BES cyber system.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Based on N&ST recommendation for a revised definition of LERC, N&ST recommends changing requirement statement 3.1 to: “For LERC, if any, permit only necessary inbound and outbound electronic access as determined by the Responsible Entity.”

Likes 0	
Dislikes 0	

Response

David Greyerbiehl - CMS Energy - Consumers Energy Company - 5

Answer	No
Document Name	

Comment
CIP-003-7 draft currently states that the Responsible Entity (RE) shall implement electronic access controls, but it does not clearly state in CIP-003 Attachment 1 Section 3.1 that electronic access controls are only required IF all three criteria is present. Please modify the CIP-003 Attachment 1 Section 3.1 to clearly state that. In addition, please consider adding a statement that if the criteria is not applicable, i.e., if there is not “a routable protocol”, the RE is not required to establish electronic access controls.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	

Comment
Based on N&ST recommendation for a revised definition of LERC, N&ST recommends changing requirement statement 3.1 to: “For LERC, if any, permit only necessary inbound and outbound electronic access as determined by the Responsible Entity.”

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment
Seminole appreciates the Standard Development Team’s work on this requirement, especially the efforts to make this a non-prescriptive risk based security standard. Seminole generally supports the revision, but suggests a minor change to clarify the requirement. While Seminole supports this component of the requirement, we suggest adding a clarification to Attachment 1, Section 3. The statement in 3.1.i “between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);” Is unclear and can be interpreted in two different ways for audit purposes. 1. If a BES Cyber Asset is present behind the firewall, all traffic must be controlled and documented; or 2. Only traffic passing through the firewall to a BES Cyber System must be controlled and documented, other traffic destined to a non-BES Cyber System does not require any controls.

Seminole recommends that suitable language be added to clarify the intent for auditing purposes. For example:

1. “between a routable network containing a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

2. “between a BES Cyber Asset contained within a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);”

Likes 0	
Dislikes 0	

Response

Yuguang Xiao - Manitoba Hydro - 5

Answer	No
Document Name	

Comment

We disagree with the language within Attachment 1 - 3.1 (i) as it applies to using the assets physical border as the defining line where electronic access controls must be deployed, as it is inconsistent with allowable solutions for higher impact levels. The asset border concept has logical consistency issues by allowing unfettered routable communication across a large site such as a generation facility, but disallowing routable communications without access controls between different assets that are close together such as a generation station and a switchyard. Suggest utilizing the concept of Electronic Security Perimeters which allows the entity to define a logical border within an asset or cross two assets like a medium impact ESP with access points deployment.

Likes 0	
Dislikes 0	

Response

Blair Mukanik - Manitoba Hydro - 6

Answer	No
Document Name	

Comment

We disagree with the language within Attachment 1 - 3.1 (i) as it applies to using the assets physical border as the defining line where electronic access controls must be deployed, as it is inconsistent with allowable solutions for higher impact levels. The asset border concept has logical consistency issues by allowing unfettered routable communication across a large site such as a generation facility, but disallowing routable communications without access controls between different assets that are close together such as a generation station and a switchyard. Suggest utilizing the concept of Electronic Security Perimeters which allows the entity to define a logical border within an asset or cross two assets like a medium impact ESP with access points deployment.

Likes 0	

Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC	
Answer	Yes
Document Name	
Comment	
Reclamation commends the SDT on this effort to simplify the standard.	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Tri-State agrees with the revisions but we recommend the SDT include an “and” at the end of i. in Attachment 1 Section 3.1. We acknowledge that there is some language in the Supplemental Material stating electronic access controls are only required for communications when all three of the criteria are met but we believe that is an important detail that should be captured in the attachment.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
See comments from #7	
Likes 0	
Dislikes 0	

Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
See comments from #7.	
Likes 0	
Dislikes 0	
Response	
Alexander Vedvik - Public Service Commission of Wisconsin - 9	
Answer	Yes
Document Name	
Comment	
However, the PSCW suggests that NERC consider comments by Manitoba Hydro and Seminole Electric Cooperative, Inc., in order to make the final revision as clear as possible to all registered entities.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	

Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees each asset containing low impact BES Cyber System(s) should be afforded electronic access controls For any communication that meets the criteria in 3.1.i-iii.	
Likes 0	
Dislikes 0	
Response	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Seattle City Light appreciates the efforts of the Standard Drafting Team to respond to comments regarding the previous draft of CIP-003-7 and is supportive of the approach taken in the present draft. That said, Seattle urges a change in the language of R3.1, to make it crystal clear that all three criteria must be satisfied in order for the obligation to apply. Seattle finds the convention to be unnecessarily confusing (because its an arcane and obscure variant of ordinary English usage) that a numbered list denotes an "and" relationship among members of the list and that a bulleted list denotes an "or" relationship. Seattle suggests the following change (additions in ALL CAPS): ***3.1** Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that SATISFY ALL THREE OF THE FOLLOWING CRITERIA:* *i. ARE between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);* *ii. USE a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and,* *iii. ARE not used for time* *ensuring protocol IEC TR* *are using protocol IEC TR-* *61850* *-90-5 R-GOOSE).*	
Likes 0	
Dislikes 0	
Response	

David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	

Comment
NYPA is NOT supportive of the proposed changes to Attachment 1-Section 3. It is confusing what is the necessary treatment for cyber assets included in a “Facility” but not a BES Cyber System. In addition the definition of terms regarding “asset”, “routable communication”, “any communication”, and “electronic access” as included in attachment 1 and the supplemental information is necessary for clarification and applicability.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	

Comment
AZPS recommends that the SDT consider adding clarity regarding routable communication between Low Impact BCSs and those Cyber Assets that are located within the same asset (facility). While the proposed requirement is clear that routable communications from a Low Impact BCS that travel outside of the asset (facility) must have electronic access controls in place, it is unclear whether there is a similar expectation for routable communication with Cyber Assets located within the same asset, but that are not associated with the Low Impact BCS. AZPS notes that the diagrams contained in the supplemental materials appear to contain some electronic controls associated with Low Impact BCS, which may be contributing to confusion and ambiguity. While we believe the current language is an improvement, AZPS may not be able to vote affirmatively on this requirement if the ambiguity is not addressed.

Likes 0	
Dislikes 0	

Response

Michael Mertz - PNM Resources - 3	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rich Hydzik - Rich Hydzik On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Rich Hydzik	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Malozewski - Hydro One Networks, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	
Document Name	
Comment	
adopt PSEG comments	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Please see Texas RE’s response to number 1.	
Likes 0	
Dislikes 0	
Response	

3. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 2 Physical Security Controls to reflect the retirement of LEAP. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
This section needs to be modified to be congruent with a LERC definition which is allows for the exception of traffic not destined for a local BES cyber system.	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
1) {C}We would like the SDT to clarify what the non-defined term “electronic access controls” means. The former definition of LEAP provided a specific definition for the controls that a low impact entity had to implement. This change introduces ambiguity into the requirements. 2) {C}We are assuming that the question refers to CIP-003-6, Attachment 1, Section 3 – rather than Section 2.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
We would like to see some additional language in the GTB to clarify that the intent is not to require a separate need justification for physical security control to the systems that provide electronic access controls. For example, in a substation, if we justify a need for a population of people who need	

access to the control house where Low BCA's are located, we would not expect to have to separately justify why that same population needs access to a device within the substation that provides electronic access controls	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
We recommend rearranging the Electronic Access Controls (currently Section 3) so that it should become Section 2 and the Physical Electronic Access Controls (currently Section 2) should become Section 3. Section 2 refers to Section 3.1 in both Attachment 1 and the Guidelines and Technical Basis and therefore it would be easier to read if the Electronic Access Controls section appeared first.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC	
Answer	Yes
Document Name	
Comment	
Reclamation commends the SDT on this effort to simplify the standard.	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	

We recommend rearranging the Electronic Access Controls (currently Section 3) so that it should become Section 2 and the Physical Electronic Access Controls (currently Section 2) should become Section 3. Section 2 refers to Section 3.1 in both Attachment 1 and the Guidelines and Technical Basis and therefore it would be easier to read if the Electronic Access Controls section appeared first.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern Company joins EEI in recommending rearranging the Electronic Access Controls (currently Section 3) so that it should become Section 2, and the Physical Access Controls (currently Section 2) as Section 3. Section 2 refers to Section 3.1 in both Attachment 1 and the Guidelines and Technical Basis and therefore it would be easier to read if the Electronic Access Controls section appeared first.

Likes 0	
Dislikes 0	

Response

Michael Mertz - PNM Resources - 3

Answer	Yes
Document Name	

Comment

We recommend rearranging the Electronic Access Controls (currently Section 3) so that it should become Section 2 and the Physical Electronic Access Controls (currently Section 2) should become Section 3. Section 2 refers to Section 3.1 in both Attachment 1 and the Guidelines and Technical Basis and therefore it would be easier to read if the Electronic Access Controls section appeared first.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Blair Mukanik - Manitoba Hydro - 6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Yuguang Xiao - Manitoba Hydro - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alexander Vedvik - Public Service Commission of Wisconsin - 9	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Malozewski - Hydro One Networks, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael DeLoach - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rich Hydzik - Rich Hydzik On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Rich Hydzik	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s response to #1.	
Likes 0	
Dislikes 0	
Response	

Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	
Document Name	
Comment	
adopt PSEG comments	
Likes 0	
Dislikes 0	
Response	

4. Attachment 2: The SDT revised the complementary language of CIP-003-6, Attachment 2, Sections 2 and 3 to make the evidential language of the measure consistent with the revised requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

In Section 3 of Attachment 2, we suggest changing the word “rationale” to “business justification.”

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC

Answer	No
Document Name	

Comment

Reclamation recommends changing Section 3 to:

Electronic Access Controls: Examples of evidence for Section 3 may include, but are

not limited to:

1. Documentation identifying required inbound and outbound traffic connections to Low Impact BES Cyber Systems (such as lists or representative diagrams.)

2. Documentation identifying access controls where routable protocols (that the Responsible Entity deems necessary) are used for inbound and outbound traffic (such as restricting IP addresses, ports, or services; authenticating users; air sessions on a non BES Cyber System; implementing unidirectional gateways, etc.)

Documentation identifying methods used to authenticate Dial-up Connectivity (such as 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, access control on the BES Cyber System, or other authentication methods.)

Likes 0	
Dislikes 0	

Response

Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
1) We have concerns that the evidence includes lists of controls that correspond to low impact assets (IP addresses, ports, gateways, etc.). Lists of low impact BES Cyber Assets are explicitly out of scope, per CIP-002. 2) If the SDT takes the approach of requiring a documented process for low impact controls, as long as the Responsible Entity is not expected to specifically diagram any low impact BES Cyber Assets, the evidence would be acceptable to allow an entity to speak to its documented electronic access control methodology.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Since we do not agree with the language pertaining to Attachment 1 we cannot support the expamples of evidince identified in Attachment 2.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
This section needs to be modified to be congruent with a LERC definition which is allows for the exception of traffic not destined for a local BES cyber system. IPC generally agrees with the language added to the actual CIP-003 standard and its associated attachments, but contends that the requirements in Attachment 1 of CIP-003 with the associated revision to LERC will in essence require a back door inventory of Low Impact BCS. It is difficult for an entity to effectively comply with Section 2 and to a lesser degree Section 3 without an inventory of Low Impact BCS. However, this directly conflicts with	

explicit language of CIP-002. The SDT needs to strongly consider revising CIP-002 in order to fix the inherent problems that it causes and that then cascades through the rest of the CIP standards and then causes all SDTs to dance around these types of issues now and in the future.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
Section 2, Item b: N&ST suggests changing “Cyber Asset” to “Cyber Asset(s)” to account for the possibility that more than one Cyber Asset is used to implement electronic access controls. Section 3: N&ST recommends minor edits reflecting N&ST-recommended revised definition of LERC.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
Section 2, Item b: N&ST suggests changing “Cyber Asset” to “Cyber Asset(s)” to account for the possibility that more than one Cyber Asset is used to implement electronic access controls. Section 3: N&ST recommends minor edits reflecting N&ST-recommended revised definition of LERC.	
Likes 0	
Dislikes 0	
Response	
Yuguang Xiao - Manitoba Hydro - 5	
Answer	No
Document Name	

Comment
During SDT meeting at MH, MH has raised a question regarding if an electronic boundary is allowable to protect low impact BCAs that are located at two BES assets such as a generation station and the switchyard, where the access points would be defined to protect this electronic boundary like a medium impact ESP. In CIP-003-7_redline guidance Section, P38 states: "When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach o making this evaluation. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s).", given to using "electronic boundary associated **asset"** rather than **assets,** it is not clear if it was intended to address MH's comment allowing an electronic boundary cross two BES assets like a medium ESP. Please clarify SDT's intention about the electronic boundary. If it is intended to only allow the electronic boundary to be defined within one BES asset, please explain why since the medium ESP is allowable to cross multiple sites.

Likes 0	
Dislikes 0	

Response

Blair Mukanik - Manitoba Hydro - 6	
Answer	No
Document Name	

Comment
During SDT meeting at MH, MH has raised a question regarding if an electronic boundary is allowable to protect low impact BCAs that are located at two BES assets such as a generation station and the switchyard, where the access points would be defined to protect this electronic boundary like a medium impact ESP. In CIP-003-7_redline guidance Section, P38 states: "When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach o making this evaluation. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s).", given to using "electronic boundary associated **asset"** rather than **assets,** it is not clear if it was intended to address MH's comment allowing an electronic boundary cross two BES assets like a medium ESP. Please clarify SDT's intention about the electronic boundary. If it is intended to only allow the electronic boundary to be defined within one BES asset, please explain why since the medium ESP is allowable to cross multiple sites.

Likes 0	
Dislikes 0	

Response

Michael Mertz - PNM Resources - 3	
Answer	Yes
Document Name	

Comment

The sentence that describes evidence that “provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices” is unclear under Attachment 2, Section 3, bullet 1. It would be helpful if the SDT provided example rationales to clarify and prevent multiple interpretations.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern Company agrees with EEI's comments noting that the sentence that describes evidence that “provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices” is unclear under Attachment 2, Section 3, bullet 1. It would be helpful if the SDT provided example rationales to clarify and prevent multiple interpretations.

Likes 0	
Dislikes 0	

Response

Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1

Answer	Yes
Document Name	

Comment

The sentence that describes evidence that “provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices” is unclear under Attachment 2, Section 3, bullet 1. It would be helpful if the SDT provided example rationales to clarify and prevent multiple interpretations.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment	
See comments from Question 7.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
See comments from Question 7.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	Yes
Document Name	
Comment	
PSEG agrees with the EEI comments.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

The sentence that describes evidence that “provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices” is unclear under Attachment 2, Section 3, bullet 1. It would be helpful if the SDT provided example rationales to clarify and prevent multiple interpretations.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	Yes
Document Name	

Comment

Section 2b. propose modified wording of:

b. The Cyber Asset specified by the Responsible Entity that provides electronic access controls implemented for Attachment 1, Section 3.1, if any.Section 3.1 - propose modified wording of:

1. Documentation such as: representative diagrams that illustrate control of inbound and outbound communications between the low impact BES Cyber Asset and the Cyber Asset outside the asset containing low impact BES Cyber Systems, or lists of implemented electronic access controls (e.g. access control lists, restricting IP addresses, ….

Likes 0	
Dislikes 0	

Response

Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

BPA supports the change to add complimentary language in Attachment 2 to further support the requirement language with examples that minimize interpretation and act as the foundation for more consistent application of the standard requirements.

Likes 0	
Dislikes 0	

Response

Rich Hydzik - Rich Hydzik On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Rich Hydzik	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael DeLoach - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Paul Malozewski - Hydro One Networks, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alexander Vedvik - Public Service Commission of Wisconsin - 9	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	
Document Name	
Comment	
adopt PSEG comments	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE will review facts and circumstances during compliance and enforcement reviews.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	

We recommend the following language change to Attachment 2, Section 3:

“showing that at each asset or group of assets containing low impact BES Cyber Systems, bi directional routable communication between a low impactBES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted byelectronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary,”

The addition of the term “bi directional” is necessary based on our concerns outlined in question 1, and would promote consistency throughout the document.

Likes 0	
Dislikes 0	

Response

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides example diagrams that illustrate various electronic access controls at a conceptual level. Do you agree with the revisied content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns

Answer	No
Document Name	

Comment

The reference models should now show the demarcation point of the electronic access control like they once did for LEAP rather than just the firewall icon.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	No
Document Name	

Comment

In Reference model 10 (page 51 of 65), Dominion recommends changing the example from TDM and SONET to “protocol independent transport”. The use of generic terminology would allow for the inclusion of MPLS, TDM, SONET, T1, DSL, etc.

Likes 0	
Dislikes 0	

Response

Blair Mukanik - Manitoba Hydro - 6

Answer	No
Document Name	

Comment

During SDT meeting at MH, MH has raised a question regarding if an electronic boundary is allowable to protect low impact BCAs that are located at two BES assets such as a generation station and the switchyard, where the access points would be defined to protect this electronic boundary like a medium impact ESP. In the guidance Section, P38 states: “When determining whether a routable protocol is entering or leaving the asset containing

the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach o making this evaluation. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s).”, given to using “electronic boundary associated **asset”** rather than **assets,** it is not clear if it was intended to address MH’s comment allowing an electronic boundary cross two BES assets like a medium ESP. Please clarify SDT’s intention about the electronic boundary. If it is intended to only allow the electronic boundary to be defined within one BES asset, please explain why since the medium ESP is allowable to cross multiple sites.

Likes 0	
Dislikes 0	

Response

Yuguang Xiao - Manitoba Hydro - 5

Answer	No
Document Name	

Comment

During SDT meeting at MH, MH has raised a question regarding if an electronic boundary is allowable to protect low impact BCAs that are located at two BES assets such as a generation station and the switchyard, where the access points would be defined to protect this electronic boundary like a medium impact ESP. In the guidance Section, P38 states: “When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach o making this evaluation. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s).”, given to using “electronic boundary associated **asset”** rather than **assets,** it is not clear if it was intended to address MH’s comment allowing an electronic boundary cross two BES assets like a medium ESP. Please clarify SDT’s intention about the electronic boundary. If it is intended to only allow the electronic boundary to be defined within one BES asset, please explain why since the medium ESP is allowable to cross multiple sites.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

The language of several Reference Models states “When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary.” This language sounds like a Requirement. Recommend striking this sentence in all locations because the diagrams should be illustrative, allowing the Responsible Entity Flexiblity to implement appropriate security controls, as provided by the Requirements language. Also recommend striking the final sentence in Reference Models 1, 2 and 3. These security ocntrols are good suggestions and could be added as suggestions at the beginning of the Guidelines and Technical Basis.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	

Comment 1:

Language provided in Reference Model 10 contains substantive impact on how entities identify traffic as routable: "In similar configurations, the Responsible Entity should closely evaluate the transport entering or leaving the asset containing low impact BES Cyber System(s). If the communication entering or leaving the asset containing low impact BES Cyber System(s) was routable (such as serial encapsulated in TCP/IP or UDP/IP as depicted Reference Model 2 or Reference Model 5), then the criteria requiring electronic access controls would be met."

Specifically, when utilizing communications circuits from a third party communications provider, an entity has no control or knowledge over the transport level technologies employed. From an entity's perspective, a 56K four-wire circuit is completely non-routable. However, the telecom provider may convert it to IP based communications in the telecom transport pathway prior to converting it back to a 56K four-wire circuit when entering a remote facility.

These transport-layer characteristics are transparent to the devices at each end of a communications link. The criteria specified in Reference Model 10 implies that potential encapsulations and conversions, outside of an entity's control (or even awareness), may qualify an otherwise non-routable communications link as routable.

As written, to verify transport level characteristics as provided in Reference Model 10 would require auditing all transport layer equipment and configurations as employed by the telecom provider.

TVA suggests that specific technical criteria that qualifies traffic as routable be included in a NERC Glossary term instead of language contained in a "Supplemental Material" section of a standard.

Comment 2:

Language provided in the section headed “Insufficient Access Controls” contains substantive impact on communication options available for use by entities: “Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include: […] A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.”

As written, the last sentence prevents the use of all internet based communications solutions that utilize a public IP address. This includes any cellular, satellite, or ISP based service. Many acceptable, and secure, internet based communications solutions exist where data can be appropriately secured. Most of these solutions would utilize some form of VPN or SSL technology. Access control is not contingent upon what IP addresses may or may not be used.

TVA recommends striking this bullet completely or clarifying the language to accommodate secure internet based communication solutions.

Likes 0	
Dislikes 0	

Response

Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
The previous version of CIP-003-7 presented examples of asset boundaries and explicitly allowed extended asset boundaries beyond the property line. In order to prevent the addition of communications control equipment without significant gain in security, we believe that the SDT should explicitly extend the asset limits provided that physical or electronic controls are in place. The diagrams should reflect this option.	
Likes 0	
Dislikes 0	
Response	

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA generally agrees with the Guidelines and Technical Basis section, but sees two items that need addressing. While the SDT acknowledged there are concerns regarding shared facilities, FMPA does not believe the revised language completely addresses those concerns. Section 2 of Attachment 1 still states "**[e]ach** Responsible Entity shall control physical access." This simply does not work at share facilities because more than one entity cannot have control at the same time. It is essential for entities with BES Cyber Systems in shared facilities to be able to enter into agreements that identify the Repsonsible Entity controlling physical access. FMPA supports Seminole Electric Cooperative, Inc.'s proposed language for addressing shared facilities. Also, Reference Models 3 and 7 use the term "Non BES Cyber System" while others use the term "Non-BES Cyber Asset". FMPA believes cyber assest more accurately reflects what these devices are and that all the models should use consistent language.	
Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	

Comment
N&ST recommends updating this section to reflect N&ST-recommended revised definition of LERC. Comments on specific reference models: N&ST believes Reference Model 6 (“Indirect Access”) is problematic in several regards. First of all, having attempted to respond to FERC’s directive to clarify what is meant by “direct” access by simply eliminating the word from CIP-003, the SDT reopens the debate by introducing the concept of “*indirect* access.” Second, N&ST believes the Reference Model’s assertion that the depicted “indirect access” “...meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset...” is incorrect if the depicted non-BES Cyber Asset is terminating the routable protocol connection between the “external” Cyber Asset and itself. N&ST recommends either eliminating this example or revising it to indicate there is *not* communication between the low impact BES Cyber System and an “external” Cyber Asset if the non-BES Cyber Asset inside the asset is providing an application-layer protocol break. If N&ST's proposed revised definition of LERC was applied to this Reference Model, N&ST believes LERC would not be present in this case. Reference Model 5 (“User Authentication”) has similar problems. Is the depicted non-BES Cyber Asset that is performing authentication continuing the same communications session from the external Cyber Asset to the low impact BES Cyber System by performing IP to serial protocol conversion, such as depicted in Reference Model 2? If so, N&ST agrees that there is communication between the low impact BES Cyber System and the external Cyber Asset. If, on the other hand, (1) the authenticating non-BES Cyber Asset is terminating the routable protocol connection from outside the asset and, (2) a user, once authenticated by that Cyber Asset, must initiate a new, serial communications session between the authenticating non-BES Cyber Asset and the low impact BES Cyber System, then N&ST believes the proposed electronic access control requirement would not be applicable. If N&ST's proposed revised definition of LERC was applied to this Reference Model, N&ST believes LERC would not be present in this case.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	

Comment
N&ST recommends updating this section to reflect N&ST-recommended revised definition of LERC. Comments on specific reference models: N&ST believes Reference Model 6 (“Indirect Access”) is problematic in several regards. First of all, having attempted to respond to FERC’s directive to clarify what is meant by “direct” access by simply eliminating the word from CIP-003, the SDT reopens the debate by introducing the concept of “*indirect* access.” Second, N&ST believes the Reference Model’s assertion that the depicted “indirect access” “...meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset...” is incorrect if the depicted non-BES Cyber Asset is terminating the routable protocol connection between the “external” Cyber Asset and itself. N&ST recommends either eliminating this example or revising it to indicate there is *not* communication between the low impact BES Cyber System and an “external” Cyber Asset if the non-BES Cyber Asset inside the asset is providing an application-layer protocol break. If N&ST's proposed revised definition of LERC was applied to this Reference Model, N&ST believes LERC would not be present in this case. Reference Model 5 (“User Authentication”) has similar problems. Is the depicted non-BES Cyber Asset that is performing authentication continuing the same communications session from the external Cyber Asset to the low impact BES Cyber System by performing IP to serial protocol conversion, such as depicted in Reference Model 2? If so, N&ST agrees that there is communication between the low impact BES Cyber System and the external Cyber Asset. If, on the other hand, (1) the authenticating non-BES Cyber Asset is terminating the routable protocol connection from outside the asset and, (2)

a user, once authenticated by that Cyber Asset, must initiate a new, serial communications session between the authenticating non-BES Cyber Asset and the low impact BES Cyber System, then N&ST believes the proposed electronic access control requirement would not be applicable. If N&ST's proposed revised definition of LERC was applied to this Reference Model, N&ST believes LERC would not be present in this case.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

This section needs to be modified to be congruent with a LERC definition which is allows for the exception of traffic not destined for a local BES cyber system. This section includes a diagrams which need modified as well. None of the reference models depict traffic crossing the asset boundary but are destined for other sites and therein lies the problem with the definition being so all inclusive.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

The language of Reference Models 1, 2 and 3 states “When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary.” MMWEC recommends striking this sentence because it contradicts Section 3 in Attachment 1 and Attachment 2, which allow flexibility in how the Responsible Entity chooses to implement access controls.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5

Answer	No

Document Name	
Comment	
The conceptual diagrams continue to appear confusing at best. We have concerns about how the GTB are factored into Compliance and Enforcement. In some cases it appears that they create “requirements” that must be incorporated into your program; this is inconsistent with prior FERC precedent. On the other hand, it is not clear whether or not you can rely on the GTB in developing your program and ensuring compliance.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	
The language of several Reference Models states “When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary.” This language sounds like a Requirement. Recommend striking this sentence in all locations because the diagrams should be illustrative, allowing the Responsible Entity Flexiblity to implement appropriate security controls, as provided by the Requirements language. Also recommend striking the final sentence in Reference Models 1, 2 and 3. These security ocntrols are good suggestions and could be added as suggestions at the beginning of the Guidelines and Technical Basis.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
We do not support the Guidelines nor Technical Basis as we do not support the language in this draft Standard.	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	

Answer	No
Document Name	
Comment	

1) {C}A Responsible Entity should be able to develop their own approach based on their unique electronic access control implementation methodology.

2) {C}The technical controls are helpful guidance, but the requirements should not require a list of low impact BES Cyber Assets.

Likes 0	
Dislikes 0	
Response	

Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC

Answer	No
Document Name	
Comment	

Under the Dial-up Connectivity section, Reclamation recommends the first paragraph be changed to:

"Dial-up Connectivity: For dial-up connectivity to a low impact BES Cyber System, the following access control methods:

1. The modem allowing access to a low impact BES Cyber System is configured to dial out only (no auto-answer) to deliver data,
2. The modem allowing access to a low impact BES Cyber System is configured as a dialback modem,
3. The modem allowing access to a low impact BES Cyber System is enabled or powered up by on-site personnel only when needed, and disabled when not in use.
4. The modem allowing access to a low impact BES Cyber System is enabled or powered up remotely from a Control Center or control room only when needed, and disabled when not in use.
5. The modem allowing access to a low impact BES Cyber System is configured for auto-answer, but the communications are encrypted, protecting Cyber Assets from unauthorized control within the low impact BES Cyber System.
6. The low impact BES Cyber System is configured with access control when accessed using Dial-up Connectivity."

Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	
Comment	
The SPP Standards Review Group requests consideration of further refinement to the language of the GTB in Requirements R1 and R2. Specific to Requirement 1, the language is not consistent with the GTB reference section to R1. Specific to Requirement 2, it is unclear which document Attachment 1 is associated with (CIP-002 or CIP-003-7).	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes the technical diversity of the examples provide sufficient guidance for consistent interpretation and application of the standard.	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
While Seminole supports the technical merits and the Guidelines and Technical Basis changes, Seminole refers the team to additional issues identified in question 7 that may best be addressed in the Guidelines and Technical Basis section of the standard.	
Likes 0	
Dislikes 0	
Response	

Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the content, however recommends that the requirement language be reviewed against the diagrams provided to ensure that there is not ambiguity or confusion created between the two portions of the standard. While we believe the current language is an improvement, AZPS may not be able to vote affirmatively on this requirement if the ambiguity is not addressed.	
Likes 0	
Dislikes 0	
Response	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Seattle in particular appreciates the addition of Reference Model 10, to illustrate the common case of a SONET system carrying both routable and non-routable traffic.	
Likes 0	
Dislikes 0	
Response	

Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP appreciates the use of example diagrams. Reference model 10 is particulary useful. However, MPLS is still not addressed within the diagrams. SRP requests the SDT create an example diagram to address MPLS as the transport network. Would only the out of band management network be considered as the electronic access or is it expected the MPLS transport connection must traverse an electronic access control such as a firewall?	
Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Under the draft, electronic access controls must be implemented for routable connections to low impact BES Cyber Systems such that only “necessary” traffic is permitted. The determination of what is “necessary” remains in the hands of the Responsible Entity, but documentation to support why communications are “necessary” would likely be required because these determinations will need to be justified. Documenting why the permitted traffic for each routable connection is “necessary” could be extremely burdensome. The GTB should explicitly allow Responsible Entities to define the necessary communications generically, so that separate documentation need not be maintained for each routable communication at each site. Propose that the GTB specifically state that the intent is not to require access control list or other line by line justifications.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
We believe that “the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level.” However, we are concerned with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says “the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process.” We also understand that at the November MRC meeting NERC Staff and the Standards Committee leadership agreed to work together on a way forward on the GTB that affords deference. EEI encourages NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.	
Likes 1	Massachusetts Municipal Wholesale Electric Company, 5, Gordon David
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	Yes
Document Name	
Comment	

PSEG agrees with the EEI comments.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

We align with Edison Electric Institute's (EEI) comments, stating:

We believe that "the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level." However, we are concerned with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says "the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process." We also understand that at the November MRC meeting NERC Staff and the Standards Committee leadership agreed to work together on a way forward on the GTB that affords deference. EEI encourages NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

We align with Edison Electric Institute's (EEI) comments, stating:

We believe that "the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level." However, we are concerned with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says "the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process." We also understand that at the November MRC meeting NERC Staff and the Standards Committee leadership agreed to work together on a way forward on the GTB that affords deference. EEI encourages NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.

Likes 0	
Dislikes 0	

Response

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Tri-State appreciates the SDT's work on the Reference Models; however, we recommend the SDT split up the three concepts displayed in Model 8. The current diagram is a bit confusing and may be misinterpreted as one combined concept, rather than three separate ones.

Tri-State would appreciate the inclusion of some examples of what equipment or configurations might qualify as a "Uni-directional Gateway". There has been a lack of consistency among regions as to what devices would apply for this designation and we would like some clarity from the SDT on this. Specifically, we wonder whether the SDT considers a properly configured firewall to be included as a part of this designation?

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern Company agrees that "the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level." However, Southern Company joins EEI in expressing concern with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says "the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process." Southern Company joins EEI to encourage NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.

Page 42 of 65, Reference Model 3: "The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be another asset containing low impact BES Cyber System(s)."

SOCO Comment: It appears this statement should read "… that may or may not be ***at*** another asset containing low impact BES Cyber System(s)." The word *"at"* appears to be missing in this statement.

Page 42 of 65, Reference Model 3: "Care should be taken that electronic access to or between each asset is through the electronic access controls at the centralized location."

SOCO Comment: Consider the following edits to this statement: “Care should be taken that electronic access to or between each asset is through the ***Cyber Asset(s) determined by the Responsible Entity to be performing/providing*** electronic access controls at the centralized location.”

Page 43 of 65, Reference Model 4: Was the term “bi-directional” intentionally struck from the requirement language? This seems to cause issues in Reference Model 4 – Uni-directional Gateway. As the modifications to the Standard are read now, inbound **OR** outbound communications to assets containing Low Impact BES Cyber Systems require protections; Section 3, 3.1 Part ii – “using a routable protocol when entering **OR** leaving the asset.” Therefore, the uni-directional gateway allowing routable communications only to flow outside of the asset containing Lows would still require protections.

Likes 0	
Dislikes 0	

Response

Michael Mertz - PNM Resources - 3

Answer	Yes
Document Name	

Comment

We believe that “the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level.” However, we are concerned with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says “the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process.” We also understand that at the November MRC meeting NERC Staff and the Standards Committee leadership agreed to work together on a way forward on the GTB that affords deference. EEI encourages NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Malozewski - Hydro One Networks, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael DeLoach - AEP - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rich Hydzik - Rich Hydzik On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Rich Hydzik	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alexander Vedvik - Public Service Commission of Wisconsin - 9	
Answer	
Document Name	
Comment	
The PSCW abstains. However, we recommend NERC consider comments by registered entities impacted by this standard.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's response to #1.	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	
Document Name	
Comment	
adopt PSEG comments	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	
Document Name	
Comment	
We believe that "the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level." However, we are concerned with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says "the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process." We also understand that at the November MRC meeting NERC Staff and the Standards Committee leadership agreed to work together on a way forward on the GTB that affords deference. EEI encourages NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.	
Likes 0	
Dislikes 0	

Response

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) date for the revisions made to CIP-003, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer, please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

Michael Mertz - PNM Resources - 3

Answer	No
Document Name	

Comment

The CIP-003-6 plan for Requirement R1, part 1.2 is due April 1, 2017, which depends on the use of LERC and LEAP, which the Commission has ordered NERC to modify.The CIP-003-7 modifications remove the use of LERC and LEAP terms. Although we agree with the modifications, we do not believe that these modifications can be made and approved by the Commission by this date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the Commission approves the modifications. We urge that NERC and FERC consider this implementation impact on Requirement R1 and recommend that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standards Review Group requests delaying the specification of an effective date until the SDT has resolved any issues within the standard.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment
Although Southern Company agrees with the proposed modifications, as noted by EEI, Southern Company does not find that these modifications can be made and approved by the Commission by the required date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the Commission approves the modifications. Southern Company joins EEI in urging that NERC and FERC consider this implementation impact on Requirement R1 and recommends that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.

Likes 0	
Dislikes 0	

Response

Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	No
Document Name	

Comment
The CIP-003-6 plan for Requirement R1, part 1.2 is due April 1, 2017, which depends on the use of LERC and LEAP, which the Commission has ordered NERC to modify. The CIP-003-7 modifications remove the use of LERC and LEAP terms. Although we agree with the modifications, we do not believe that these modifications can be made and approved by the Commission by this date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the Commission approves the modifications. We urge that NERC and FERC consider this implementation impact on Requirement R1 and recommend that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.

Likes 0	
Dislikes 0	

Response

Rich Hydzik - Rich Hydzik On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Rich Hydzik	
Answer	No
Document Name	

Comment
The CIP-003-6 plan for Requirement R1, part 1.2 is due April 1, 2017, which depends on the use of LERC and LEAP, which the Commission has ordered NERC to modify. The CIP-003-7 modifications remove the use of LERC and LEAP terms. Although we agree with the modifications, we do not believe that these modifications can be made and approved by the Commission by this date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the Commission approves the modifications. We urge that NERC and FERC consider this implementation impact on Requirement R1 and recommend that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.

Likes 0	

Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC	
Answer	No
Document Name	
Comment	
Reclamation recommends a more achievable implementation plan of 24 months from the date of FERC approval.	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
1) The implementation plan should not occur until 2019. We do not support the proposed target date of September 1, 2018, because there are several other requirements that already will go into effect on this date. The burden of compliance with this proposal would add significant resources and costs with implementing these low impact security measures, especially for smaller entities. 2) The implementation plan should allow for an additional budgeting cycle to ensure industry has time to implement such controls.	
Likes 0	
Dislikes 0	
Response	
Michael DeLoach - AEP - 3	
Answer	No
Document Name	
Comment	
Twelve months is insufficient time to react to the extremely large number of assets containing low impact BES Cyber Systems. AEP has almost 2000. This is only the first of several potential revisions to CIP-003 necessary to completely address FERC Order 829??. Two years is probably	

needed to fully comply with this the first of several revisions CIP-003. The hope is that twelve months will accommodate all the revisions of CIP-003 resulting from the Order. This is consistant with the original allowance in the CIP-003-5 implementation plan that was approved. Lets do it once.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion

Answer	No
Document Name	

Comment

Due to budget cycles and quantity of equipment that must be installed, we propose keeping the language included in the “General Consideration” section but extend the interval from 12 months to 18 months.

Likes 0	
Dislikes 0	

Response

Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame

Answer	No
Document Name	

Comment

1. The implementation plan should not occur until 2019. We do not support the proposed target date of September 1, 2018, because there are several other requirements that already will go into effect on this date. The burden of compliance with this proposal would add significant resources and costs with implementing these low impact security measures, especially for smaller entities.

2. The implementation plan should allow for an additional budgeting cycle to ensure industry has time to implement such controls.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker

Answer	No
Document Name	

Comment
While we appreciate the increase of over 9 months included in the original posting, we believe that 12 months is insufficient for the successful implementation of these requirements. Through the inclusion of indirect communications now being required to meet the security objective of implementing electronic access controls that permit only necessary inbound and outbound access, the SDT has substantially increased the evidentiary burden to document the controls implemented for this use case. Given the large volume of assets at low impact, 12 months is not long enough to properly implement this revised control. We understand that the SDT has extended its planned implementation plan for Transient Cyber Assets at low impact to 18 months and believe that the implementation timeline for the LERC requirements should also be adjusted to 18 months. This will allow sufficient time for LERC implementation and allow for operational efficiencies to occur by implementing the LERC requirements and the TCA requirements concurrently.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	

Comment
We align with Edison Electric Institute's (EEI) comments, stating: *The CIP-003-6 plan for Requirement R1, part 1.2 is due April 1, 2017, which depends on the use of LERC and LEAP, which the Commission has ordered NERC to modify. The CIP-003-7 modifications remove the use of LERC and LEAP terms. Although we agree with the modifications, we do not believe that these modifications can be made and approved by the Commission by this date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the Commission approves the modifications. We urge that NERC and FERC consider this implementation impact on Requirement R1 and recommend that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.*

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	

Comment
See EEI comments

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

Comments: We align with Edison Electric Institute's (EEI) comments, stating:

The CIP-003-6 plan for Requirement R1, part 1.2 is due April 1, 2017, which depends on the use of LERC and LEAP, which the Commission has ordered NERC to modify. The CIP-003-7 modifications remove the use of LERC and LEAP terms. Although we agree with the modifications, we do not believe that these modifications can be made and approved by the Commission by this date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the Commission approves the modifications. We urge that NERC and FERC consider this implementation impact on Requirement R1 and recommend that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

We suggest extending the proposed implementation time-period for electronic and physical access controls by revising the wording to: "later of April 1, 2019 or the first day of .....". The transition to CIP Version 5/6 utilized significant entity resources during the past two years. Given that Low Impact BES Cyber Systems pose a lower risk to system reliability (by definition), we submit that allowing additional time is reasonable and would allow entities time to better integrate this work with other priorities.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No

Document Name	

Comment

Revising standards and then expecting the industry to change directions and then comply with the requirements in the same amount of time is not a feasible approach. Although the depth of requirements associated with Low Impact BCS is less compared to the High and Medium BCS the breadth of what it will encompass is much greater. Entities have had to halt or slow the progress on their approach considering the changes to LERC, which is a major component to CIP-003. As these sections of CIP-003 had a later implementation due to their newness and scope and now there are major changes to how they will be approached there is no reason why the implementation schedule can't be moved by at least 6 to 12 months which will be the amount of time from when the standards went into effect (7/1/2016) and when FERC will hopefully approves them (2nd or 3rd Qtr of 2017.) I would propose the implementation date be the later of either April 1, 2019 or July 1 ,2019 or 12 months from the date of approval.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

NRECA appreciates the efforts of the SDT to address the comments from the previous draft. However, we believe that 12 months is not an adequate amount of time to complete the implementation of these revised requirements. Through the inclusion of indirect communications now being required to meet the security objective of implementing electronic access controls that permit only necessary inbound and outbound access, the SDT has substantially increased the evidentiary burden to document the controls implemented for this use case. Given the large volume of assets at low impact, 12 months is not long enough to properly implement this revised control. We understand that the SDT has extended its planned implementation plan for Transient Cyber Assets at low impact to 18 months and believe that the implementation timeline for the LERC requirements should also be adjusted to 18 months. This will allow sufficient time for LERC implementation and allow for operational efficiencies to occur by implementing the LERC requirements and the TCA requirements concurrently.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG

Answer	No
Document Name	

Comment

PSEG agrees with the EEI comments.

Likes 0	
Dislikes 0	
Response	
Ronnie Frizzell - Arkansas Electric Cooperative Corporation - 4	
Answer	No
Document Name	
Comment	
I agree with the comments from NRECA	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The CIP-003-6 plan for Requirement R1, part 1.2 is due April 1, 2017, which depends on the use of LERC and LEAP, which the Commission has ordered NERC to modify. The CIP-003-7 modifications remove the use of the LERC and LEAP terms. Although we agree with the modifications, we do not believe that these modifications can be made and approved by the Commission by this date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the Commission approves the modifications. We urge that NERC and FERC consider this implementation impact on Requirement R1 and recommend that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	

Due to budget cycles and quantity of equipment that must be installed, we propose keeping the language included in the “General Consideration” section but extend the interval from 12 months to 18 months.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

The CIP requirements for low impact BES Cyber Systems are currently in flux and entities will not have certainty regarding low impact requirements until they are approved by the Commission. In addition, the sheer number of assets containing low impact BES Cyber Systems is substantial. It will take entities time to implement proper physical and electronic access controls at all the various locations. CenterPoint Energy believes it is reasonable to request additional time to implement the requirements given that the facilities are low risk to the reliability of the BES. CenterPoint Energy recommends the effective date for CIP-003-7 revisions to be delayed 18 months after FERC approval.

Additionally, CenterPoint Energy agrees with EEI’s comments to align the implementation date of CIP-003-6 R1, Part 1.2.2 and 1.2.3 (cyber security policies) with the effective date of the LERC changes to Attachment 1, Section 2 and Section 3 (cyber security plans). Although CenterPoint Energy supports the retirement of the LERC/LEAP terms in CIP-003-7, the LERC/LEAP terms are still used in the currently approved CIP-003-6 requirements that are effective April 1, 2017. Therefore, entities will need to comply with two versions of the CIP-003 standard between April 1, 2017 and the effective date of version 7. This could cause entities substantial rework and resource constraints because what is being implemented is a moving target. It will be more efficient and effective for entities to implement one version of the standard and align their cyber security policies with the cyber security plans for requirement CIP-003-7, Attachment 1, Section 2 and Section 3.

Likes 0	
Dislikes 0	

Response

Philip Huff - Arkansas Electric Cooperative Corporation - 3

Answer	No
Document Name	

Comment

AECC supports the comments submitted by NRECA.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Process development and implementation of Low BCS electronic access controls has been significantly delayed and remains contingent upon requirements finalization. Propose allowance of a minimum of 24 months from FERC approval date to compliance date for CIP-003-7 R2, Attachment 1 Sections 2 and 3.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

Due to budget cycles and quantity of equipment that must be installed, we propose keeping the language included in the “General Consideration” section but extend the interval from 12 months to 18 months.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	No
Document Name	

Comment

For the implementation plan which is 12 months, Dominion recommends an 18 month implementation period for the following reasons:

- Time is needed for entities to assess and confirm indirect access as an acceptable access control.
- New environments may be in scope.

- While this revision approach is more consistent with the currently approved CIP version6 requirements, the revisions necessitate that entities conduct an impact assessment to determine what changes the revisions create and what is currently in place from the assesments performed for CIP version 6 implementation.
- Revision iterations always require some time to assess and verify points of change.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy does not disagree with the proposed Implementation Plan. The changes proposed will prompt entities to go back and review their planning and implementation for CIP-003-6, and revise accordingly. The extra time to review and potentially change operating processes and plans is necessary.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	Yes
Document Name	

Comment

Did the SDT intend to modify the enforceability of CIP-003-6 via this Implementation Plan? If so, FMPA recommends the addition in bold to the language below.

“The Responsible Entity shall not be required to include in its cyber security plan(s) elements related to Sections 2 and 3 of **CIP-003-6** Attachment 1 until the effective date of CIP-003-7.”

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Procurement, design, installation, and configuration of electronic access controls.	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA supports this timeline. Site inventories and the work to develop scope for new programs to meet the standard requirements will require time to approve, develop and implement a sustainable compliance program.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	

Answer	Yes
Document Name	
Comment	
OPG is in the process of surveying all of its Low Impact Rating BES assets to determine where there is communication between the asset or a Low Impact BES Cyber Asset within the asset with an external Cyber Asset. If the communication is using a routable protocol then the appropriate electronic security controls are being selected and installed to permit only neccessary inbound and outbound electronic access.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Yuguang Xiao - Manitoba Hydro - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Blair Mukanik - Manitoba Hydro - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	
Document Name	
Comment	
adopt PSEG comments	
Likes 0	

Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE respectfully requests the SDT provide a basis for its decision to adopt a 12-month compliance window, including any data it considered in determining that this was an appropriate window for affected entities to meet their compliance obligations under the revised Standards. Texas RE requests the revised implementation plan clarify Section 4, 4.5; the testing the Cyber Security Incident response plan(s). There is confusion amongst the Industry on whether the plan must be tested on or before April 1, 2017, or 36 calendar months after the effective date.	
Likes 0	
Dislikes 0	
Response	
Alexander Vedvik - Public Service Commission of Wisconsin - 9	
Answer	
Document Name	
Comment	
The PSCW abstains.	
Likes 0	
Dislikes 0	
Response	

7. If you have additional comments on the proposed revisions to address the FERC directive regarding the LERC definition that you have not provided in response to the questions above, please provide them here.

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	
Document Name	

Comment

Thank you for retiring this definition.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns

Answer	
Document Name	

Comment

ITC Holdings does not agree with changing the ‘Guidelines and Technical Basis’ (GTB) document to ‘Supplemental Material’. Changing the name of the document does not solve any of the issues regarding whether or not regions will uphold it – it only causes more confusion. The ballot body approves the GTB as part of the standard and it should be agreed to by all regions to ensure there is consistency in how the GTB is treated.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC

Answer	
Document Name	

Comment

No comments at this time.

Likes 0	
Dislikes 0	

Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	
Document Name	
Comment	
Dominion requests that NERC petition FERC to delay and/or cancel CIP-003-6 (in a similar manner to version 4) until the currently approved CIP version is superseded by CIP version 7. Requiring Registered Entities to identify and document LERCs and LEAPs only to remove those requirements is an unreasonable burden and does not contribute to the reliable operation of the BES.	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	
Document Name	
Comment	
Seminole appreciates the Standard Development Team's work on this requirement, especially the efforts to make this a non-prescriptive risk based security standard. While Seminole currently supports the Guidelines and Technical Basis section related to the diagrams, there are additional issues to address and, therefore, Seminole is voting no on the current ballot. The term asset is an undefined term. This term is a core component of the requirement. Without a definition or guidance within the document clarifying the intent of the term asset, it is likely that in certain cases audit teams and entities will interpret this term differently. Elimination of the phrase asset boundary reduces but does not eliminate this concern. The term asset should be addressed with a section in the Guidelines and Technical Basis. For example, It should be clarified whether the term asset refers to the entire location, the components within the location that contains a BES Cyber System, or to Cyber Assets and other Facilities, systems, and equipment within that location "owned by each Responsible Entity in Section 4.1" (CIP-003 section 4.2- Applicability). However, any changes should be carefully considered with respect to CIP-002-5.1. Seminole continues to have concerns that assets with multiple entities having Cyber Assets in a single location is not adequately addressed. This is a particularly important topic in the FRCC region due to the high number of Transmission Operators that are interconnected in a small region. It is common that shared facilities such as substations with interconnections and substations owned by Distribution Providers to have multiple entities with Cyber Assets within a single control house. While the currently recommended approach is a Memorandum of Understanding, this approach leaves multiple entities at risk of a violation if the asset owner fails to provide appropriate physical security. Seminole recommends language similar to the following be placed in the Guidelines and Technical Basis section of the Standard to clarify the role of the Memorandum of Understanding: "In cases where multiple entities have a Cyber Asset located that are protected in a common location and the security is provided by one entity, a signed and dated agreement such as a Memorandum of Understanding between the Cyber Asset(s) owner and the entity providing physical security sufficiently documents the specific party responsible for meeting physical security requirements."	
Likes 1	Gowder Chris On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins,

Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
Seattle has one additional concern, that the approach to routable connectivity expressed in the present draft does not address the issue of mixed communications paths involving both routable and non-routable communications. As written, it appears that so long as a non-routable communications segment crosses the border of the BES asset containing the Low impact BES Cyber System, the entire system is judged to communicate non-routably. Although this is a simple and clear approach, it seems to conflict with the more nuanced approaches urged over the years since 2009 by FERC and regional regulators regarding the differentiation between external routable communications and non-routable communications. Seattle understands that another group from the CIP v7 Drafting Team is developing a revised approach to External Routable Connectivity that considers the nuances of mixed communications modes. As such, Seattle is concerned that when that effort is complete, CIP-003-7 R2 Attachment 1 Item 3.1 will require revision (again) to reflect that change—and it will come after entities have implemented their communications controls for their Low assets. Seattle urges that the two efforts be aligned to minimize the chance of such a change and the attendant additional effort and expense that may be required to change, again, compliance programs, documentation, and actual field communication installations.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	

Reference Model 8: The term “air gap” may not be universally understood and goes undefined in the standard. A pure reading of air gap is that there is no connectivity at all to the device. However, in a substation it is common to have contact oriented connected, while not serial or Ethernet, there is still a cable connected and therefore not a pure “air gap.” Exelon recommends replacing the use of “air gap” with “physical isolation from routable protocol” or using a red circle to depict no communication as in Reference Model 3 to be consistent with title and text of Reference Model 8.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	

Comment

CenterPoint Energy is in favor of filing the TCA modifications and implementation plan with the LERC modifications, if possible.

Likes 0	
Dislikes 0	

Response

Roger Dufresne - Hydro-Qu?bec Production - 5

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	
Document Name	

Comment
Based on our understanding from reading the requirements. Removing the terms LERC and LEAP doesn't remove the efforts required to implement and maintain low impact systems.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	

Comment
CIP Exceptional Circumstances has not been included within CIP-003-7 as drafted. CIP exceptional circumstances should be included as a provision for Low Impact Entities and therefore considered in this standard.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	

Comment
The intent of these revisions are understood and are an improvement for cyber security around BES Cyber Assets. Minnesota Power has concerns surrounding the lack of clarity as to how Registered Entities will comply with the Standard. The CIP Standards family has become more prescriptive over time (specifically the auditing approach by the Regional Entities), this Standard seems to be moving in a different direction, becoming less prescriptive and open. Though this approach is appreciated, NERC must provide clear guidance to the regional entities for auditing, in a consistent manner, to the Standard’s intentions.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	

Document Name	
Comment	
The intent of these revisions are understood and are an improvement for cyber security around BES Cyber Assets. Minnesota Power has concerns surrounding the lack of clarity as to how Registered Entities will comply with the Standard. The CIP Standards family has become more prescriptive over time (specifically the auditing approach by the Regional Entities), this Standard seems to be moving in a different direction, becoming less prescriptive and open. Though this approach is appreciated, NERC must provide clear guidance to the regional entities for auditing, in a consistent manner, to the Standard's intentions.	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	
Document Name	
Comment	
None at this time.	
Likes 0	
Dislikes 0	
Response	
Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame	
Answer	
Document Name	
Comment	
We urge the SDT to stagger its posting schedule so different drafts of the CIP standards do not have overlapping deadlines to submit comments. Industry is currently focused on implementing the existing CIP V5 standards, while also paying attention to the development of these revisions. There should not be multiple deadlines assigned to this project, as this creates a strain on CIP subject matter experts to review and provide feedback on the proposed changes.	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	
Document Name	
Comment	
no comments	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	
Document Name	
Comment	
adopt PSEG comments	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	

Answer	
Document Name	
Comment	

We urge the SDT to stagger its posting schedule so different drafts of the CIP standards do not have overlapping deadlines to submit comments. Industry is currently focused on implementing the existing CIP V5 standards, while also paying attention to the development of these revisions. There should not be multiple deadlines assigned to this project, as this creates a strain on CIP subject matter experts to review and provide feedback on the proposed changes.

We thank you for this opportunity to comment.

Likes 0	
Dislikes 0	
Response	

Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC

Answer	
Document Name	
Comment	

Due to the existing order to enforce CIP-003-6 with the LERC and LEAP definitions, Reclamation recommends to skip the CIP-003-6 enforcement and combine the changes to CIP-003-7 and CIP-003-TCA into CIP-003-7.

Likes 0	
Dislikes 0	
Response	

Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1

Answer	
Document Name	
Comment	

None

Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2016-02 Modifications to CIP Standards | CIP-003-7 and Implementation Plan
Comment Period Start Date:	10/21/2016
Comment Period End Date:	12/5/2016
Associated Ballots:	2016-02 Modifications to CIP Standards CIP-003-7 AB 2 ST 2016-02 Modifications to CIP Standards CIP-003-7 Implementation Plan AB 2 OT 2016-02 Modifications to CIP Standards CIP-003-7 Non-binding Poll AB 2 NB

There were 61 sets of responses, including comments from approximately 136 different people from approximately 108 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Director of Standards Development, Steve Noess (via email) or at (404) 446-9691.

Questions

1. Definition: The SDT is proposing the retirement of the terms Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP). The SDT incorporated the LERC concepts into the Requirement R2 language and removed the LERC reference from Requirement R1, Part 1.2.3 and the LEAP references from Attachment 1, Sections 2 and 3.1. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

2. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 3 to require each Responsible Entity to implement electronic access controls for each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002 that permit only necessary inbound and outbound electronic access as determined by the Responsible Entity. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

3. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 2 Physical Security Controls to reflect the retirement of LEAP. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

4. Attachment 2: The SDT revised the complementary language of CIP-003-6, Attachment 2, Sections 2 and 3 to make the evidential language of the measure consistent with the revised requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides example diagrams that illustrate various electronic access controls at a conceptual level. Do you agree with the revisied content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) date for the revisions made to CIP-003, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer, please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

7. If you have additional comments on the proposed revisions to address the FERC directive regarding the LERC definition that you have not provided in response to the questions above, please provide them here.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Chris Gowder	Chris Gowder		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utility Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steve Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Mark Brown	City of Winter Park	4	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	9	FRCC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
ACES Power Marketing	Colleen Campbell	6	NA - Not Applicable	ACES Standards Collaborators	Shari Heino	Brazos Electric Power Cooperative, Inc.	1,5	Texas RE
					John Shaver	Arizona Electric Power Cooperative, Inc.	1	WECC
					Mike Brytowski	Great River Energy	1,3,5,6	MRO
					Ryan Strom	Buckeye Power, Inc	4	RF
					Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	RF
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Watson	Old Dominion Electric Cooperative	3,4	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Wes Moody	East Kentucky Power Cooperative	1,3	SERC
					Paul Mehlhaff	Sunflower Electric Power Corporation	1,5	SPP RE
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,10	NPCC	RSC no Dominion	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					David Ramkalawan	Ontario Power Generation	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Chuck Lawrence	American Transmission Company	1	MRO
					Chuck Wicklund	Otter Tail Power Company	1,5	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Shannon Weaver	Midcontinent Independent System Operator	2	MRO
					Brad Parret	Minnesota Power	1,5	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Tony Eddleman	Nebraska Public Power District	1,3,5	MRO
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Louis Guidry	Cleco Power	1,3,5,6	SPP RE
					Steve Keller	Southwest Power Pool Inc	2	SPP RE
					Robert Hirchak	Cleco Power	1,3,5,6	SPP RE
Public Service Enterprise Group	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF

Summary of Changes

CIP-003-7:

Based on stakeholder comments, the SDT made non-substantive changes to the standard, primarily in the Guidelines and Technical Basis section to provide additional clarity.

Implementation Plan:

Based on stakeholder comments, the SDT lengthened the implementation period from twelve (12) calendar months to eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard. This non-substantive change rendered the September 1, 2018 date moot; consequently, it was removed.

1. Definition: The SDT is proposing the retirement of the terms Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP). The SDT incorporated the LERC concepts into the Requirement R2 language and removed the LERC reference from Requirement R1, Part 1.2.3 and the LEAP references from Attachment 1, Sections 2 and 3.1. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	

Comment

N&ST appreciates the SDT's efforts to address Order 822's directive to add clarity to the definition of LERC. However, we believe that simply retiring the term will not adequately resolve the fundamental question of when, and under what conditions, electronic access controls (draft CIP-003-7 Attachment 1 Section 3) must be applied in order to protect low impact BES Cyber Systems (see N&ST comments on "Guidelines and Technical Basis," following). Accordingly, N&ST suggests taking advantage of the existing, industry, NERC and FERC approved of "External Routable Connectivity" and modifying it for low impact as follows: LERC = "The ability to access a low impact BES Cyber System from a Cyber Asset that is outside of the BES asset in which it is contained via a bi-directional routable protocol connection." The exception for point-to-point connections between IEDs for time-sensitive control and protection functions can be retained from the original LERC definition. N&ST wishes to point out this proposed definition does not in any way introduce the concept of an Electronic Security Perimeter to low impact environments, which is something that FERC has indicated it is presently not inclined to require (Order 822, paragraph 75).

N&ST agrees with the proposed retirement of the term, "LEAP."

Likes 0	
Dislikes 0	

Response

While adding the ERC language to the LERC definition is consistent with existing language, the SDT asserts that the new criteria drafted in CIP-003 Attachment 1, Section 3 provide more clarity and definition as to when electronic access controls are required.

David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	No
Document Name	
Comment	
CIP-003-7 draft currently states that the Responsible Entity (RE) shall implement electronic access controls, but it does not clearly state in CIP-003 Attachment 1 Section 3.1 that electronic access controls are only required IF all three criteria is present. Please modify the CIP-003 Attachment 1 Section 3.1 to clearly state that. In addition, please consider adding a statement that if the criteria is not applicable, i.e., if there is not “a routable protocol”, the RE is not required to establish electronic access controls.	
Likes 0	
Dislikes 0	
Response	
The SDT asserts that proper application of the three scoping criteria in CIP-003-7, Attachment 1, Section 3 adhering to requirement 2 achieves the same result as stating the negative.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST appreciates the SDT’s efforts to address Order 822’s directive to add clarity to the definition of LERC. However, we believe that simply retiring the term will not adequately resolve the fundamental question of when, and under what conditions, electronic access controls (draft CIP-003-7 Attachment 1 Section 3) must be applied in order to protect low impact BES Cyber Systems (see N&ST comments on “Guidelines and Technical Basis,” following). Accordingly, N&ST suggests taking advantage of the existing, industry, NERC and FERC approved of “External Routable Connectivity” and modifying it for low impact as follows: LERC = “The ability to access a low impact BES Cyber System from a Cyber Asset that is outside of the BES asset in which it is contained via a bi-directional routable protocol connection.” The exception for point-to-point connections between IEDs for time-sensitive control and protection functions can be	

retained from the original LERC definition. N&ST wishes to point out this proposed definition does not in any way introduce the concept of an Electronic Security Perimeter to low impact environments, which is something that FERC has indicated it is presently not inclined to require (Order 822, paragraph 75).

N&ST agrees with the proposed retirement of the term, “LEAP.”

Likes 0	
Dislikes 0	

Response

While adding the ERC language to the LERC definition is consistent with existing language, the SDT asserts that the new criteria drafted in CIP-003 Attachment 1, Section 3 provide more clarity regarding when electronic access controls are required.

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

The description of the current draft states:

"The SDT simplified Section 3 of Attachment 1 to require the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the exclusion language (previously in the definition of LERC) contained in (iii) which reads: “not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R- GOOSE)”."

This unnecessarily includes all communications traffic which may not even be destined for a BES cyber system at that site. As a matter of normal operation our internal communications network switches traffic through site which are not the final destination for the

traffic. This new definition would bring all of that traffic unnecessarily into scope. Even if the requirements to adhere to the applicable standard are low, Idaho Power will be spend unnecessary dollars on keep track of and report on this. The definition should be modified to only include traffic destined for a local BES cyber system. An additional exception stating "excluding traffic not destined for a local BES cyber system." The SDT does not seem to understand that not all traffic crossing an asset boundary is destined for that asset, some traffic may continue on from the asset to other assets. Traffic destined for other assets should not be controlled and specifically permitted at every stop along the way. It should be controlled at the communications ingress and egress points only.

Likes 0	
Dislikes 0	

Response
The SDT cannot comment on whether any particular implementation would be compliant with the language of the drafted requirements. The determination of whether electronic access controls are required must be based upon the specific facts and circumstances of the Responsible Entity's implementation, including the specific network design for the low impact BES Cyber Systems. That said, the SDT notes that Attachment 1, Section 3 specifies the application of electronic access controls be performed for "each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002." Further, the communications requiring electronic access controls must meet the simultaneous application of the three criteria specified in Attachment 1, Section 3.1. The SDT intends for the "asset" referenced in Section 3.1 under romanettes i and ii to be the same asset for which the implementation of electronic access controls is performed. Communications which are not destined for a low impact BES Cyber System are intended to be excluded.

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. – 5	
Answer	No
Document Name	

Comment
While the revisions to CIP-003 obviate the need for the problematice LERC and LEAP definitions, they retain some of the ambiguity regarding physical versus logical characteristics. Suggested revision:

"3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any user-intiated communications that are: i. between a low impact BES Cyber System(s) and an external network(s) or a Cyber Asset(s) residing outside of a network to which low impact BES Cyber System(s) are connected; ii. using a routable protocol when entering or leaving the network on which the low impact BES Cyber System(s) reside; and, iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)."	
Likes 0	
Dislikes 0	
Response	
The SDT disagrees with the addition of "user-initiated" for communications. The SDT asserts that both user-initiated and machine-to-machine communication(s) present risks to the low impact BES Cyber System(s) that necessitate the implementation of electronic access controls. The requirement language does not prescribe a physical versus logical approach to the implementation. The use of the term "asset" refers to assets identified as containing low impact BES Cyber System(s) pursuant to CIP-002. As described in the G&TB, the Responsible Entity has the flexibility to identify the electronic boundary surrounding the low impact BES Cyber System rather than using a physical boundary.	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy requests further clarification from the SDT regarding the removal of the term "bi directional"from Section 3 in Attachment 1. Is it the SDT's interpretation that the term "bi directional" was redundant, and thus not necessary in the language? The term "bi	

directional" is not included in the definition of "Routable Protocol," and removing the term in this instance promotes ambiguity, and could impact applicability of the standard.	
Likes 0	
Dislikes 0	
Response	
The SDT asserts that controls which enforce one-way communications are themselves among the electronic access controls that should be implemented in a manner to meet the security objective outlined in Attachment 1, Section 3. Consequently, the SDT disagrees that the term bi-directional should be included in the language.	
Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
1) The SDT's approach to retire the definitions of LERC and LEAP by implementing low impact electronic access controls is one way to address the directive in FERC Order No. 822, which focused on the ambiguity of the word "direct." However, this approach creates unintended consequences for compliance. In particular, the proposed revisions implicitly require low impact entities to have an identified list of low impact assets, which is specifically excluded in CIP-002. 2) The SDT's proposed approach will create difficulty for both industry to demonstrate compliance and for auditors to determine reasonable assurance. 3) We suggest the SDT consider another method to address the FERC directive that still preserves the low impact requirements and the explicit exclusion from being required to have an inventory list of low impact assets. 4) One possible approach is for low impact entities to have a documented process that applies electronic access controls to low impact assets. a. Auditors could verify that the entity has developed the documented process, and the entity could demonstrate compliance by providing the document as evidence.	

b. This approach also preserves the disparate treatment of low and medium impact assets, by assigning different levels of requirements that are commensurate with the risks they pose to the Bulk Electric System.	
Likes 0	
Dislikes 0	
Response	
The SDT contends that a list of low impact BES Cyber Systems is not required to demonstrate compliance with the requirement. Requirement R2 is a plan-based requirement, and evidence to demonstrate compliance is based on content in its plan. The SDT suggests that Responsible Entities review the G&TB, the RSAW, and corresponding measure(s) for additional information. The SDT appreciates the suggestion, but does not think that only having a process to implement electronic access controls provides sufficient clarity to Responsible Entities regarding when electronic access controls are necessary.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
As the SDT doesn't appear to have made any changes to R2, we are confused as to how LERC concepts were incorporated via only the removal of the defined terms. The retirement of the terms Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) provides less clarity in the information addressing electronic access controls in section R1 - 1.2.3. Also, R1.2 mentions assets identified in CIP-002 and low impact BES Cyber Systems. However, it is unclear whether the parts listed below (Parts 1.2.1 - 1.2.4) are creating requirements associated with CIP-002 or CIP-003-7. Changing "specified" to "identified" in the following: "and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." will make the electronic access device more clearly defined by the entity.	

Likes 0	
Dislikes 0	
Response	
The clarity provided is not solely in the removal of the defined terms, but also in the addition of language to Attachment 1, Section 3 which provides specific criteria for communications where electronic access controls are required. The term “LERC” was only used within CIP-003.	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
LADWP technical standards and policies for equipment and infrastructure inherently provide the security attributes required by the proposed changes to CIP-003-7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA supports the retirement of LERC and LEAP and the removal of references in Attachment 1.	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
City Light has no comments for Q1	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the removal of the terms LERC and LEAP and appreciates the SDT for simplifying the requirement language. After reviewing where the language was replaced, SRP agrees with the verbiage used to substitute the terms. Additionally, SRP appreciates the removal of the use of asset boundary from the language. The requirements are much clearer than before.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
The concepts that replaced the Defined Terms are an improvement from the previous definitions for LERC and LEAP. The new concept puts emphasis in protecting BES Cyber Assets, but lacks clarity on how compliance with the Standard will be achieved.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
The concepts that replaced the Defined Terms are an improvement from the previous definitions for LERC and LEAP. The new concept puts emphasis in protecting BES Cyber Assets, but lacks clarity on how compliance with the Standard will be achieved.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC	
Answer	Yes
Document Name	
Comment	
Reclamation commends the SDT on this effort to simplify the standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Blair Mukanik - Manitoba Hydro - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Yuguang Xiao - Manitoba Hydro - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Alexander Vedvik - Public Service Commission of Wisconsin - 9	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Hydro One Networks, Inc., 3, Malozewski Paul
Dislikes 0	
Response	
Paul Malozewski - Hydro One Networks, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael DeLoach - AEP - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rich Hydzik - Rich Hydzik On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Rich Hydzik	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Michael Mertz - PNM Resources - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE appreciates the SDT's continued efforts to develop a workable definition of Low Impact External Routable Connectivity (LERC) that addresses FERC's directive in Order No. 822. As FERC's directive made clear, the focus of this project should be on developing a workable modification to the LERC definition consistent with "the commentary in the Guidelines and Technical Basis section of CIP-003-6." In fulfilling this mandate, the SDT has elected to retire the LERC definition and instead incorporate elements of the LERC and Low-Impact BES Cyber System Electronic Access Point (LEAP) concepts into a new requirement focused on electronic access controls. While the SDT's approach appears to also meet the terms of the FERC directive, Texas RE remains concerned that introducing such new

concepts may lead to confusion. Given this fact, Texas RE continues to believe that the better approach is to draw from facility Electronic Access Point concepts already set forth in CIP-005. As such, Texas RE proposes the following revision to Attachment 2, Section 3.1 in lieu of the SDT's current approach: *Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default."*. With this change, Texas RE's proposed Section 3.1 would read as follows:

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber

System(s) identified pursuant to CIP-002, the Responsible Entity shall implement

electronic access controls to:

3.1 *Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default* for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and,

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Texas RE believes that such an approach would make the CIP Standards more consistent with one another while avoiding introducing new and untested concepts in a project designed to have a limited scope.

Texas RE acknowledges that FERC did not direct NERC to utilize the concept of Electronic Security Perimeters for low impact systems and to leverage existing definitions for EAP and ERC. However, given the approach taken by the SDT in response to FERC's narrow directive, Texas RE believes that the SDT may wish to consider extending the familiar concepts in the existing ERC definition to the LERC environment at this juncture as part of the developing a new electronic access control requirements.

Likes 0	
Dislikes 0	

Response
The SDT strives to create consistency and clarity with any new elements added to the CIP standards. Due to the significant diversity in asset types at low impact, the SDT determined that mirroring the requirements from CIP-005 did not provide the best approach for requiring electronic access controls at low impact. Rather, the SDT contends that the new criteria drafted in CIP-003 Attachment 1, Section 3 provide more clarity regarding when electronic access controls are required over using existing language from medium and high impact.

Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	
Document Name	
Comment	
adopt PSEG comments	
Likes 0	
Dislikes 0	
Response	

2. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 3 to require each Responsible Entity to implement electronic access controls for each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002 that permit only necessary inbound and outbound electronic access as determined by the Responsible Entity. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
We suggest the SDT re-evaluate the electronic access control is required. We feel that the electronic access control should be applied to each of the low impact BES Cyber System(s) in the identified asset containing low impact BES Cyber Assets instead of the asset that contains the low impact Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
The SDT acknowledges that this is a valid option to meet the requirement. The standard provides flexibility in how to implement the requirements, as explained in the G&TB.	
Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	

1) This requirement suggests that Responsible Entities must identify or otherwise list their low impact Cyber Assets similar in nature to a medium-impact requirement; otherwise how will compliance be evaluated? This approach contradicts CIP-002, which states an inventory list of low impact BES Cyber Systems (or Cyber Assets) is not required.

2) Responsible Entities are *only* required to implement electronic access controls to assets containing low impact BES Cyber Systems with *necessary* inbound and outbound electronic access. There does not appear to be much clarity around the criteria for access "necessity" and therefore the benchmark for the requirement of implementing electronic access controls is unclear and unmeasurable. How will compliance with this be evaluated?

3) Consider requiring a documented methodology for implementing electronic access controls for each asset containing low impact BES Cyber Systems.

a. This alleviates any implied requirement for maintaining an inventory list of low impact assets, and would allow the Responsible Entity to incorporate use of exclusion criteria to those communications it deems applicable.

Likes 0	
Dislikes 0	

Response

) The SDT contends that a list of low impact BES Cyber Systems is not required to demonstrate compliance with the requirement. Requirement R2 is a plan-based requirement, and evidence to demonstrate compliance is based on content in its plan. The SDT suggests that Responsible Entities review the G&TB, the RSAW, and corresponding measure(s) for additional information.

2) The necessity of access must be evaluated by the Responsible Entity, and adding a clear definition of 'necessary' might seem desirable but may reduce flexibility. The SDT does not believes creating a standard-specific definition for this term is the best way of enhancing the standard with clarity and guidance.

3) The G&TB section lists several options for electronic access controls. Demonstration of compliance is not required to be performed at the cyber asset level.

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	No
Document Name	
Comment	
SMUD/BANC is not supportive of the proposed changes to Attachment 1-Section 3. It is confusing what is the necessary treatment for cyber assets included in a "Facility" but not a BES Cyber System. In addition the definition of terms regarding "asset", "routable communication", "any communication", and "electronic access" as included in attachment 1 and the supplemental information is necessary for clarification and applicability.	
Likes 0	
Dislikes 0	
Response	
The necessity of access is evaluated by Responsible Entity. The expectation is that the entity will document the rationale that the access control meets the security objective. Adding a clear definition of these terms might seem desirable. The SDT does not believe creating standard-specific definitions for these terms is the best way of enhancing the standard with clarity and guidance. These terms do not require a NERC Glossary definition because they do not have a meaning that is different from what is found within a standard English dictionary.	
Michael DeLoach - AEP – 3	
Answer	No
Document Name	
Comment	
Question is not written consistant with the proposed Section 2 language. The electronic access controls are to be applied to the external (to the asset) routable communications from/to low impact BES Cyber Systems not all routable communications to the asset.	

Comments: The wording under Section 3 item ii brings into scope every routable connection that enters or leaves an asset containing low impact BES Cyber System. This is an overly broad classification and reaches beyond the regulation of equipment involved in the operation of the BES. There can be multiple routable conections into and out of an asset containing low impact BES Cyber Ssytems that provide no connection to low impact BES Cyber Assets. Item ii should be removed from Section 3.	
Likes 0	
Dislikes 0	
Response	
For an external routable connection to be brought into scope, it would have to meet the three criteria of paragraph 3.1 (i and ii and iii). Therefore communication to non BES cyber systems are out of scope	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy recommends the following language change to Attachment 1, Section 3.1 i: *"between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset, as determined by the Responsible Entity, containing low impact BES Cyber System(s);"* We feel that the addition of "as determined by the Responsible Entity" is necessary in that it reduces ambiguity, and promotes consistency with other aspects of this section.	
Likes 0	
Dislikes 0	
Response	
The SDT asserts that the proposed addition does not reduce ambiguity.	

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	No
Document Name	
Comment	
Please see above comments regarding physical and logical characteristics.	
Likes 0	
Dislikes 0	
Response	
We appreciate the comment, the SDT believes the proposed language sufficiently addresses the FERC order. The SDT disagrees with the addition of "user-initiated" for communications. The SDT asserts that both user-initiated and machine-to-machine communication(s) present risks to the low impact BES Cyber System(s) that necessitate the implementation of electronic access controls.	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
MMWEC is voting to approve with the following comment: MMWEC recommends changing the proposed CIP-003-7 Attachment 1, Section 3.1(ii) to the following: "ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber Systems(s) or using a routable protocol when the BES Cyber Asset is addressable using a routable protocol from outside the asset; and,"	

Rationale As currently written the criteria in Attachment 1, Section 3.1 for requiring electronic access controls would exempt communication to a BES Cyber Asset that uses an IP to serial protocol converter if that converter is located outside of the asset and only serial communications enter the asset. This would be the case even if the protocol converter faces the public Internet. The GTB (p. 33) states that entities can "identify an 'electronic boundary' associated with the asset." Thus, an entity could designate the electronic boundary to be between the BES Cyber Asset and the protocol converter in order to assert that there is no routable communications crossing the electronic boundary. Although compliant, this would not be secure, since the BES Cyber Asset would be addressable from a Cyber Asset located outside the asset. The recommended change to Section 3.1(ii) would reduce the risk of BES Cyber Assets that are connected to the Internet by a protocol converter from being identified by tools such as Shodan.	
Likes 0	
Dislikes 0	
Response	
While we appreciate the comment, the SDT asserts the proposed language, specifically the section "considerations for determining routable protocol communication" in the G&TB, sufficiently clarify the intent and therefore no additional clarification is needed to address the FERC order.	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
This section needs to be modified to be congruent with a LERC definition which is allows for the exception of traffic not destined for a local BES cyber system.	
Likes 0	

Dislikes 0	
Response	
The SDT appreciates your comment. Please see the SDT's response to your comment in question 1.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
Based on N&ST recommendation for a revised definition of LERC, N&ST recommends changing requirement statement 3.1 to: "For LERC, if any, permit only necessary inbound and outbound electronic access as determined by the Responsible Entity."	
Likes 0	
Dislikes 0	
Response	
The SDT asserts that the new criteria drafted in CIP-003 Attachment 1, Section 3 provide more clarity regarding when electronic access controls are required.	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	No
Document Name	
Comment	
CIP-003-7 draft currently states that the Responsible Entity (RE) shall implement electronic access controls, but it does not clearly state in CIP-003 Attachment 1 Section 3.1 that electronic access controls are only required IF all three criteria is present. Please modify the CIP-	

003 Attachment 1 Section 3.1 to clearly state that. In addition, please consider adding a statement that if the criteria is not applicable, i.e., if there is not “a routable protocol”, the RE is not required to establish electronic access controls.	
Likes 0	
Dislikes 0	
Response	
For an external routable connection to be brought into scope, it would have to meet the three criteria of paragraph 3.1 (i and ii and iii), therefore communication to non BES cyber systems are out of scope. Throughout all Reliability Standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are linked with an “and.”	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
Based on N&ST recommendation for a revised definition of LERC, N&ST recommends changing requirement statement 3.1 to: “For LERC, if any, permit only necessary inbound and outbound electronic access as determined by the Responsible Entity.”	
Likes 0	
Dislikes 0	
Response	
The SDT asserts that the new criteria drafted in CIP-003 Attachment 1, Section 3 provide more clarity regarding when electronic access controls are required.	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No

Document Name	
Comment	
Seminole appreciates the Standard Development Team's work on this requirement, especially the efforts to make this a non-prescriptive risk based security standard. Seminole generally supports the revision, but suggests a minor change to clarify the requirement. While Seminole supports this component of the requirement, we suggest adding a clarification to Attachment 1, Section 3. The statement in 3.1.i "between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);" Is unclear and can be interpreted in two different ways for audit purposes. 1. If a BES Cyber Asset is present behind the firewall, all traffic must be controlled and documented; or 2. Only traffic passing through the firewall to a BES Cyber System must be controlled and documented, other traffic destined to a non-BES Cyber System does not require any controls. Seminole recommends that suitable language be added to clarify the intent for auditing purposes. For example: 1. "between a routable network containing a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s); 2. "between a BES Cyber Asset contained within a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);"	
Likes 0	
Dislikes 0	
Response	
For an external routable connection to be brought into scope, it would have to meet the three criteria of paragraph 3.1 (i and ii and iii), therefore communication to non BES cyber systems are out of scope.	

Throughout all Reliability Standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are linked with an “and.”	
Yuguang Xiao - Manitoba Hydro - 5	
Answer	No
Document Name	
Comment	
We disagree with the language within Attachment 1 - 3.1 (i) as it applies to using the assets physical border as the defining line where electronic access controls must be deployed, as it is inconsistent with allowable solutions for higher impact levels. The asset border concept has logical consistency issues by allowing unfettered routable communication across a large site such as a generation facility, but disallowing routable communications without access controls between different assets that are close together such as a generation station and a switchyard. Suggest utilizing the concept of Electronic Security Perimeters which allows the entity to define a logical border within an asset or cross two assets like a medium impact ESP with access points deployment.	
Likes 0	
Dislikes 0	
Response	
The requirement is plan-based which allows the entity to determine what is inside and outside the asset, and subsequently implement the appropriate access control(s) that provide a sufficient level of protection to each low impact BCS contained within the asset(s). Although CIP-002 provides for the distinct identification of the asset(s) containing low impact BES Cyber System(s), there is no part of CIP-003 that precludes the entity from utilizing the same physical and electronic access controls for asset(s) at the same location. If implemented properly, this will not change the impact rating of the BES Cyber System(s). However, entities should be cautious not to create a shared BES Cyber System, which could affect the impact rating.	
Blair Mukanik - Manitoba Hydro - 6	
Answer	No
Document Name	

Comment	
We disagree with the language within Attachment 1 - 3.1 (i) as it applies to using the assets physical border as the defining line where electronic access controls must be deployed, as it is inconsistent with allowable solutions for higher impact levels. The asset border concept has logical consistency issues by allowing unfettered routable communication across a large site such as a generation facility, but disallowing routable communications without access controls between different assets that are close together such as a generation station and a switchyard. Suggest utilizing the concept of Electronic Security Perimeters which allows the entity to define a logical border within an asset or cross two assets like a medium impact ESP with access points deployment.	
Likes 0	
Dislikes 0	
Response	
The requirement is plan-based which allows the entity to determine what is inside and outside the asset, and subsequently implement the appropriate access control(s) that provide a sufficient level of protection to each low impact BCS contained within the asset(s). Although CIP-002 provides for the distinct identification of the asset(s) containing low impact BES Cyber System(s), there is no part of CIP-003 that precludes the entity from utilizing the same physical and electronic access controls for asset(s) at the same location. If implemented properly, this will not change the impact rating of the BES Cyber System(s). However, entities should be cautious not to create a shared BES Cyber System, which could affect the impact rating.	
Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC	
Answer	Yes
Document Name	
Comment	
Reclamation commends the SDT on this effort to simplify the standard.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comment.	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Tri-State agrees with the revisions but we recommend the SDT include an “and” at the end of i. in Attachment 1 Section 3.1. We acknowledge that there is some language in the Supplemental Material stating electronic access controls are only required for communications when all three of the criteria are met but we believe that is an important detail that should be captured in the attachment.	
Likes 0	
Dislikes 0	
Response	
Throughout all Reliability Standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are linked with an “and.”	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
See comments from #7	
Likes 0	
Dislikes 0	

Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
See comments from #7.	
Likes 0	
Dislikes 0	
Response	
Alexander Vedvik - Public Service Commission of Wisconsin - 9	
Answer	Yes
Document Name	
Comment	
However, the PSCW suggests that NERC consider comments by Manitoba Hydro and Seminole Electric Cooperative, Inc., in order to make the final revision as clear as possible to all registered entities.	
Likes 0	
Dislikes 0	
Response	
Refer to PSCW and Manitoba answers	

Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees each asset containing low impact BES Cyber System(s) should be afforded electronic access controls For any communication that meets the criteria in 3.1.i-iii.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Seattle City Light appreciates the efforts of the Standard SDT to respond to comments regarding the previous draft of CIP-003-7 and is supportive of the approach taken in the present draft. That said, Seattle urges a change in the language of R3.1, to make it crystal clear that all three criteria must be satisfied in order for the obligation to apply. Seattle finds the convention to be unnecessarily confusing (because its an arcane and obscure variant of ordinary English usage) that a numbered list denotes an "and" relationship among members of the list and that a bulleted list denotes an "or" relationship. Seattle suggests the following change (additions in ALL CAPS): ***3.1*** *Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that SATISFY ALL THREE OF THE FOLLOWING CRITERIA:* *i. ARE between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);* *ii. USE a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and,* *iii. ARE not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE).*	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Paragraph 6 of the CIP-003-7 standard details the use of bulleted or numbered items: Throughout all Reliability Standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are linked with an "and."	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	

Comment	
NYPA is NOT supportive of the proposed changes to Attachment 1-Section 3. It is confusing what is the necessary treatment for cyber assets included in a “Facility” but not a BES Cyber System. In addition the definition of terms regarding “asset”, “routable communication”, “any communication”, and “electronic access” as included in attachment 1 and the supplemental information is necessary for clarification and applicability.	
Likes 0	
Dislikes 0	
Response	
The necessity of access is evaluated by responsible entity. The expectation is that the entity will document the rationale that the access control meets the security objective. Adding a clear definition of those terms might seem desirable, nevertheless, those terms being well defined industry terms, the SDT does not believes adding a standard specific definition for those terms is the best way of enhancing the standard with clarity and guidance.	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
AZPS recommends that the SDT consider adding clarity regarding routable communication between Low Impact BCSs and those Cyber Assets that are located within the same asset (facility). While the proposed requirement is clear that routable communications from a Low Impact BCS that travel outside of the asset (facility) must have electronic access controls in place, it is unclear whether there is a similar expectation for routable communication with Cyber Assets located within the same asset, but that are not associated with the Low Impact BCS. AZPS notes that the diagrams contained in the supplemental materials appear to contain some electronic controls associated with Low Impact BCS, which may be contributing to confusion and ambiguity. While we believe the current language is an improvement, AZPS may not be able to vote affirmatively on this requirement if the ambiguity is not addressed.	
Likes 0	

Dislikes 0	
Response	
Access control for routable communication(s) between non-BES Cyber Asset(s) and low impact BES Cyber System(s) within the same asset is not a requirement. Low impact BES Cyber System(s) that communicate only internally within the asset(s) are not subject to the requirement. See reference model 9.	
Michael Mertz - PNM Resources - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rich Hydzik - Rich Hydzik On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Rich Hydzik	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Paul Malozewski - Hydro One Networks, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	
Document Name	
Comment	
adopt PSEG comments	
Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's response to number 1.	
Likes 0	
Dislikes 0	
Response	

3. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 2 Physical Security Controls to reflect the retirement of LEAP. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
This section needs to be modified to be congruent with a LERC definition which is allows for the exception of traffic not destined for a local BES cyber system.	
Likes 0	
Dislikes 0	
Response	
In the last posting, the SDT removed the requirement to address communication not destined to the low impact BES Cyber System. The exception for traffic not destined to a local BES Cyber Systems is shown in Reference Model 8.	
Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	

1) {C}We would like the SDT to clarify what the non-defined term “electronic access controls” means. The former definition of LEAP provided a specific definition for the controls that a low impact entity had to implement. This change introduces ambiguity into the requirements.

2) {C}We are assuming that the question refers to CIP-003-6, Attachment 1, Section 3 – rather than Section 2.

Likes 0	
Dislikes 0	

Response

Adding a clear definition of those terms might seem desirable, nevertheless, those terms being well defined industry terms, the SDT does not believe adding a standard specific definition for those terms is the best way of enhancing the standard with clarity and guidance.

The SDT contends that providing specific definitions for commonly understood words and/or terms within a standard is not necessary, and would not enhance the existing clarity of the standard.

A defined term is not used to allow an entity flexibility in implementation of the requirement.
Electronic access controls are mechanisms to meet the security objective of allowing only necessary inbound and outbound traffic. Examples of electronic access controls are contained within the reference models in the G&TB.

Chris Scanlon - Exelon - 1

Answer	Yes
Document Name	

Comment

We would like to see some additional language in the GTB to clarify that the intent is not to require a separate need justification for physical security control to the systems that provide electronic access controls. For example, in a substation, if we justify a need for a population of people who need access to the control house where Low BCA's are located, we would not expect to have to separately justify why that same population needs access to a device within the substation that provides electronic access controls

Likes 0	
Dislikes 0	
Response	
The G&TB was modified to address the recommendation. The language in the G&TB provides for responsible entities to document and implement physical security controls to low impact BES Cyber System(s) and to systems that provide electronic access control. If the systems inherit controls, noting this to avoid duplication is allowed.	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
We recommend rearranging the Electronic Access Controls (currently Section 3) so that it should become Section 2 and the Physical Electronic Access Controls (currently Section 2) should become Section 3. Section 2 refers to Section 3.1 in both Attachment 1 and the Guidelines and Technical Basis and therefore it would be easier to read if the Electronic Access Controls section appeared first.	
Likes 0	
Dislikes 0	
Response	
The order is consistent with the currently approved version of CIP-003. Reordering these sections may cause Responsible Entities to modify their existing plans and processes. The SDT contends that this would force an undue burden on entities thus declines to make the suggested modifications.	
Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC	
Answer	Yes
Document Name	
Comment	

Reclamation commends the SDT on this effort to simplify the standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
We recommend rearranging the Electronic Access Controls (currently Section 3) so that it should become Section 2 and the Physical Electronic Access Controls (currently Section 2) should become Section 3. Section 2 refers to Section 3.1 in both Attachment 1 and the Guidelines and Technical Basis and therefore it would be easier to read if the Electronic Access Controls section appeared first.	
Likes 0	
Dislikes 0	
Response	
The order is consistent with the currently approved version of CIP-003. Reordering these sections may cause Responsible Entities to modify their existing plans and processes. The SDT contends that this would force an undue burden on entities thus declines to make the suggested modifications.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	

Comment	
Southern Company joins EEI in recommending rearranging the Electronic Access Controls (currently Section 3) so that it should become Section 2, and the Physical Access Controls (currently Section 2) as Section 3. Section 2 refers to Section 3.1 in both Attachment 1 and the Guidelines and Technical Basis and therefore it would be easier to read if the Electronic Access Controls section appeared first.	
Likes 0	
Dislikes 0	
Response	
The order is consistent with the currently approved version of CIP-003. Reordering these sections may cause Responsible Entities to modify their existing plans and processes. The SDT contends that this would force an undue burden on entities thus declines to make the suggested modifications.	
Michael Mertz - PNM Resources - 3	
Answer	Yes
Document Name	
Comment	
We recommend rearranging the Electronic Access Controls (currently Section 3) so that it should become Section 2 and the Physical Electronic Access Controls (currently Section 2) should become Section 3. Section 2 refers to Section 3.1 in both Attachment 1 and the Guidelines and Technical Basis and therefore it would be easier to read if the Electronic Access Controls section appeared first.	
Likes 0	
Dislikes 0	
Response	
The order is consistent with the currently approved version of CIP-003. Reordering these sections may cause Responsible Entities to modify their existing plans and processes. The SDT contends that this would force an undue burden on entities thus declines to make the suggested modifications.	

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Blair Mukanik - Manitoba Hydro - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Yuguang Xiao - Manitoba Hydro - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alexander Vedvik - Public Service Commission of Wisconsin - 9	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Malozewski - Hydro One Networks, Inc. - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Michael DeLoach - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rich Hydzik - Rich Hydzik On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Rich Hydzik	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Please see Texas RE's response to #1.	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	
Document Name	
Comment	
adopt PSEG comments	
Likes 0	
Dislikes 0	
Response	

4. Attachment 2: The SDT revised the complementary language of CIP-003-6, Attachment 2, Sections 2 and 3 to make the evidential language of the measure consistent with the revised requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	

Comment	
In Section 3 of Attachment 2, we suggest changing the word “rationale” to “business justification.”	
Likes 0	
Dislikes 0	

Response	
A commenter suggested that Attachment 2, Section 3 should be revised to change the term “rationale” to business justification. The SDT notes that business justification is not present in CIP-005 or CIP-007 and that the current language is aligned with those standards.	
Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC	
Answer	No
Document Name	
Comment	
Reclamation recommends changing Section 3 to: Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to: 1. Documentation identifying required inbound and outbound traffic connections to Low Impact BES Cyber Systems (such as lists or representative diagrams.) 2. Documentation identifying access controls where routable protocols (that the Responsible Entity deems necessary) are used for inbound and outbound traffic (such as restricting IP addresses, ports, or services; authenticating users; air-gapping networks; terminating routable protocol sessions on a non-BES Cyber Asset; implementing unidirectional gateways, etc.)	

Documentation identifying methods used to authenticate Dial-up Connectivity (such as 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, access control on the BES Cyber System, or other authentication methods.)	
Likes 0	
Dislikes 0	
Response	
3.1. Documentation such as representative diagrams that illustrate control of inbound and outbound communications between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s), or lists of implemented electronic access controls (e.g. access control lists, restricting IP addresses, ports, or services; implementing unidirectional gateways) showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices; and 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 BES Cyber System).	
Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
1) We have concerns that the evidence includes lists of controls that correspond to low impact assets (IP addresses, ports, gateways, etc.). Lists of low impact BES Cyber Assets are explicitly out of scope, per CIP-002. 2) If the SDT takes the approach of requiring a documented process for low impact controls, as long as the Responsible Entity is not expected to specifically diagram any low impact BES Cyber Assets, the evidence would be acceptable to allow an entity to speak to its documented electronic access control methodology.	
Likes 0	

Dislikes 0	
Response	
In response to the revised draft of CIP-003-7, commenters expressed concerns that Attachment 2, Section 3 would require Responsible Entities to establish and maintain lists of Low Impact BES Cyber Systems, which appears to be in conflict with CIP-002-5.1 Part 1.3. CIP-002-5.1 Part 1.3 requires each responsible entity to "Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required)." The Standard SDT (SDT) asserts that Attachment 1, Section 3 requires Responsible Entities to implement electronic access controls for each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002. Accordingly, the Responsible Entity must provide documentation demonstrating that electronic access controls have been implemented to permit only necessary inbound and outbound electronic access as determined by the Responsible Entity. Evidence can include representative diagrams or lists of implemented electronic access controls for each asset or group of assets. The SDT asserts that this measure does not require the Responsible Entity to document a list of Low Impact BES Cyber Systems within each identified asset.	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Since we do not agree with the language pertaining to Attachment 1 we cannot support the expamples of evidince identified in Attachment 2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No

Document Name	
Comment	
This section needs to be modified to be congruent with a LERC definition which is allows for the exception of traffic not destined for a local BES cyber system. IPC generally agrees with the language added to the actual CIP-003 standard and its associated attachments, but contends that the requirements in Attachment 1 of CIP-003 with the associated revision to LERC will in essence require a back door inventory of Low Impact BCS. It is difficult for an entity to effectively comply with Section 2 and to a lesser degree Section 3 without an inventory of Low Impact BCS. However, this directly conflicts with explicit language of CIP-002. The SDT needs to strongly consider revising CIP-002 in order to fix the inherent problems that it causes and that then cascades through the rest of the CIP standards and then causes all SDTs to dance around these types of issues now and in the future.	
Likes 0	
Dislikes 0	
Response	
The SDT appreciates your comment. Please see the SDT's response to your comment in question 1 for additional information about excluding traffic not destined for a local BES Cyber System. The SDT contends that a list of low impact BES Cyber Systems is not required to demonstrate compliance with the requirement. Requirement R2 is a plan-based requirement and evidence to demonstrate compliance is based on content in its plan. The SDT suggests that Responsible Entities review the G&TB, the RSAW, and the corresponding measure(s) for additional information.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

Section 2, Item b: N&ST suggests changing “Cyber Asset” to “Cyber Asset(s)” to account for the possibility that more than one Cyber Asset is used to implement electronic access controls. Section 3: N&ST recommends minor edits reflecting N&ST-recommended revised definition of LERC.	
Likes 0	
Dislikes 0	
Response	
Commenters expressed concerns that Attachment 2, Section 2, bullet B should be modified from the singular form of Cyber Asset to the term Cyber Asset(s) in order to account for the possibility that more than one Cyber Asset can be utilized to implement required electronic access controls. The SDT reviewed this suggested revision and modified the measure language accordingly.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
Section 2, Item b: N&ST suggests changing “Cyber Asset” to “Cyber Asset(s)” to account for the possibility that more than one Cyber Asset is used to implement electronic access controls. Section 3: N&ST recommends minor edits reflecting N&ST-recommended revised definition of LERC.	
Likes 0	
Dislikes 0	
Response	
Commenters expressed concerns that Attachment 2, Section 2, bullet B should be modified from the singular form of Cyber Asset to the term Cyber Asset(s) in order to account for the possibility that more than one Cyber Asset can be utilized to implement required electronic access controls. The SDT reviewed this suggested revision and modified the measure language accordingly.	

Yuguang Xiao - Manitoba Hydro - 5	
Answer	No
Document Name	
Comment	
During SDT meeting at MH, MH has raised a question regarding if an electronic boundary is allowable to protect low impact BCAs that are located at two BES assets such as a generation station and the switchyard, where the access points would be defined to protect this electronic boundary like a medium impact ESP. In CIP-003-7_redline guidance Section, P38 states: "When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach o making this evaluation. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s).", given to using "electronic boundary associated **asset"** rather than **assets,** it is not clear if it was intended to address MH's comment allowing an electronic boundary cross two BES assets like a medium ESP. Please clarify SDT's intention about the electronic boundary. If it is intended to only allow the electronic boundary to be defined within one BES asset, please explain why since the medium ESP is allowable to cross multiple sites.	
Likes 0	
Dislikes 0	
Response	
The requirement is plan-based which allows the entity to determine what is inside and outside the asset, and subsequently implement the appropriate access control(s) that provide a sufficient level of protection to each low impact BCS contained within the asset(s). Although CIP-002 provides for the distinct identification of the asset(s) containing low impact BES Cyber System(s), there is no part of CIP-003 that precludes the entity from utilizing the same physical and electronic access controls for asset(s) at the same location. If implemented properly, this will not change the impact rating of the BES Cyber System(s). However, entities should be cautious not to create a shared BES Cyber System, which could affect the impact rating.	
Blair Mukanik - Manitoba Hydro - 6	
Answer	No

Document Name	
Comment	
During SDT meeting at MH, MH has raised a question regarding if an electronic boundary is allowable to protect low impact BCAs that are located at two BES assets such as a generation station and the switchyard, where the access points would be defined to protect this electronic boundary like a medium impact ESP. In CIP-003-7_redline guidance Section, P38 states: "When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach o making this evaluation. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s).", given to using "electronic boundary associated **asset"** rather than **assets,** it is not clear if it was intended to address MH's comment allowing an electronic boundary cross two BES assets like a medium ESP. Please clarify SDT's intention about the electronic boundary. If it is intended to only allow the electronic boundary to be defined within one BES asset, please explain why since the medium ESP is allowable to cross multiple sites.	
Likes 0	
Dislikes 0	
Response	
The requirement is plan-based which allows the entity to determine what is inside and outside the asset, and subsequently implement the appropriate access control(s) that provide a sufficient level of protection to each low impact BCS contained within the asset(s). Although CIP-002 provides for the distinct identification of the asset(s) containing low impact BES Cyber System(s), there is no part of CIP-003 that precludes the entity from utilizing the same physical and electronic access controls for asset(s) at the same location. If implemented properly, this will not change the impact rating of the BES Cyber System(s). However, entities should be cautious not to create a shared BES Cyber System, which could affect the impact rating.	
Michael Mertz - PNM Resources - 3	
Answer	Yes
Document Name	
Comment	

The sentence that describes evidence that “provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices” is unclear under Attachment 2, Section 3, bullet 1. It would be helpful if the SDT provided example rationales to clarify and prevent multiple interpretations.

Likes 0	
Dislikes 0	

Response
Commenters expressed concerns that the phrase, “provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices” is unclear and requested example rationales to provide clarification. The SDT contends that Page 33 of the Guidelines and Technical Basis (GTB) section provides additional guidance related to the electronic access control exclusion. The GTB refers to time-sensitive functions as, “…functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls.” Additionally, the GTB includes an example of excluded time-sensitive communications such as communications which may necessitate the tripping of a breaker within a few cycles. Responsible Entities can utilize the information provided in the GTB in order to appropriately identify time-sensitive functions and to document the exclusion rationale.

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	

Comment
Southern Company agrees with EEI's comments noting that the sentence that describes evidence that “provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices” is unclear under Attachment 2, Section 3, bullet 1. It would be helpful if the SDT provided example rationales to clarify and prevent multiple interpretations.

Likes 0	
Dislikes 0	
Response	
Commenters expressed concerns that the phrase, “provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices” is unclear and requested example rationales to provide clarification. The SDT contends that Page 33 of the Guidelines and Technical Basis (GTB) section provides additional guidance related to the electronic access control exclusion. The GTB refers to time-sensitive functions as, “…functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls.” Additionally, the GTB includes an example of excluded time-sensitive communications such as communications which may necessitate the tripping of a breaker within a few cycles. Responsible Entities can utilize the information provided in the GTB in order to appropriately identify time-sensitive functions and to document the exclusion rationale.	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
The sentence that describes evidence that “provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices” is unclear under Attachment 2, Section 3, bullet 1. It would be helpful if the SDT provided example rationales to clarify and prevent multiple interpretations.	
Likes 0	
Dislikes 0	
Response	
Commenters expressed concerns that the phrase, “provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices” is unclear and requested example rationales to provide clarification. The SDT contends	

that Page 33 of the Guidelines and Technical Basis (GTB) section provides additional guidance related to the electronic access control exclusion. The GTB refers to time-sensitive functions as, "…functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls." Additionally, the GTB includes an example of excluded time-sensitive communications such as communications which may necessitate the tripping of a breaker within a few cycles. Responsible Entities can utilize the information provided in the GTB in order to appropriately identify time-sensitive functions and to document the exclusion rationale.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
See comments from Question 7.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
See comments from Question 7.	
Likes 0	

Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	Yes
Document Name	
Comment	
PSEG agrees with the EEI comments.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
The sentence that describes evidence that “provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices” is unclear under Attachment 2, Section 3, bullet 1. It would be helpful if the SDT provided example rationales to clarify and prevent multiple interpretations.	
Likes 0	
Dislikes 0	

Response
Commenters expressed concerns that the phrase, “provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices” is unclear and requested example rationales to provide clarification. The SDT contends that Page 33 of the Guidelines and Technical Basis (GTB) section provides additional guidance related to the electronic access control exclusion. The GTB refers to time-sensitive functions as, “…functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls.” Additionally, the GTB includes an example of excluded time-sensitive communications such as communications which may necessitate the tripping of a breaker within a few cycles. Responsible Entities can utilize the information provided in the GTB in order to appropriately identify time-sensitive functions and to document the exclusion rationale.

Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Section 2b. propose modified wording of: b. The Cyber Asset specified by the Responsible Entity that provides electronic access controls implemented for Attachment 1, Section 3.1, if any.Section 3.1 - propose modified wording of: 1. Documentation such as: representative diagrams that illustrate control of inbound and outbound communications between the low impact BES Cyber Asset and the Cyber Asset outside the asset containing low impact BES Cyber Systems, or lists of implemented electronic access controls (e.g. access control lists, restricting IP addresses, ….	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments, the SDT has reviewed your proposed revisions and will incorporate revised language in Sections 2b and 3 of Attachment 2.	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA supports the change to add complimentary language in Attachment 2 to further support the requirement language with examples that minimize interpretation and act as the foundation for more consistent application of the standard requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rich Hydzik - Rich Hydzik On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Rich Hydzik	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael DeLoach - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Malozewski - Hydro One Networks, Inc. - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Alexander Vedvik - Public Service Commission of Wisconsin - 9	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	

Document Name	
Comment	
adopt PSEG comments	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE will review facts and circumstances during compliance and enforcement reviews.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	

We recommend the following language change to Attachment 2, Section 3:

"showing that at each asset or group of assets containing low impact BES Cyber Systems, bi directional routable communication between a low impactBES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted byelectronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary,"

The addition of the term "bi directional" is necessary based on our concerns outlined in question 1, and would promote consistency throughout the document.

Likes 0	
Dislikes 0	

Response

A commenter had concerns that the term "bi-directional" was not included in Attachment 2, Section 3. The SDT asserts that controls which enforce one-way communications are themselves among the electronic access controls that could be implemented to meet the security objective outlined in Attachment 1, Section 3. Consequently, the SDT disagrees that the term bi-directional should be included in this language.

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides example diagrams that illustrate various electronic access controls at a conceptual level. Do you agree with the revisied content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	No
Document Name	
Comment	
The reference models should now show the demarcation point of the electronic access control like they once did for LEAP rather than just the firewall icon.	
Likes 0	
Dislikes 0	
Response	
The SDT agrees and has updated the reference model diagrams with cyber assets performing electronic access controls.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	
In Reference model 10 (page 51 of 65), Dominion recommends changing the example from TDM and SONET to “protocol independent transport”. The use of generic terminology would allow for the inclusion of MPLS, TDM, SONET, T1, DSL, etc.	

Likes 0	
Dislikes 0	
Response	
The SDT agrees and has updated the G&TB.	
Blair Mukanik - Manitoba Hydro - 6	
Answer	No
Document Name	
Comment	
During SDT meeting at MH, MH has raised a question regarding if an electronic boundary is allowable to protect low impact BCAs that are located at two BES assets such as a generation station and the switchyard, where the access points would be defined to protect this electronic boundary like a medium impact ESP. In the guidance Section, P38 states: "When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach o making this evaluation. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s).", given to using "electronic boundary associated **asset"** rather than **assets,** it is not clear if it was intended to address MH's comment allowing an electronic boundary cross two BES assets like a medium ESP. Please clarify SDT's intention about the electronic boundary. If it is intended to only allow the electronic boundary to be defined within one BES asset, please explain why since the medium ESP is allowable to cross multiple sites.	
Likes 0	
Dislikes 0	
Response	
The requirement is plan-based which allows the entity to determine what is inside and outside the asset, and subsequently implement the appropriate access control(s) that provide a sufficient level of protection to each low impact BCS contained within the asset(s). Although CIP-002 provides for the distinct identification of the asset(s) containing low impact BES Cyber System(s), there is no part of CIP-003 that precludes the entity from utilizing the same physical and electronic access controls for asset(s) at the same location. If	

implemented properly, this will not change the impact rating of the BES Cyber System(s). However, entities should be cautious not to create a shared BES Cyber System, which could affect the impact rating.	
Yuguang Xiao - Manitoba Hydro - 5	
Answer	No
Document Name	
Comment	
During SDT meeting at MH, MH has raised a question regarding if an electronic boundary is allowable to protect low impact BCAs that are located at two BES assets such as a generation station and the switchyard, where the access points would be defined to protect this electronic boundary like a medium impact ESP. In the guidance Section, P38 states: "When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach o making this evaluation. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s).", given to using "electronic boundary associated **asset"** rather than **assets,** it is not clear if it was intended to address MH's comment allowing an electronic boundary cross two BES assets like a medium ESP. Please clarify SDT's intention about the electronic boundary. If it is intended to only allow the electronic boundary to be defined within one BES asset, please explain why since the medium ESP is allowable to cross multiple sites.	
Likes 0	
Dislikes 0	
Response	
The requirement is plan-based which allows the entity to determine what is inside and outside the asset, and subsequently implement the appropriate access control(s) that provide a sufficient level of protection to each low impact BCS contained within the asset(s). Although CIP-002 provides for the distinct identification of the asset(s) containing low impact BES Cyber System(s), there is no part of CIP-003 that precludes the entity from utilizing the same physical and electronic access controls for asset(s) at the same location. If implemented properly, this will not change the impact rating of the BES Cyber System(s). However, entities should be cautious not to create a shared BES Cyber System, which could affect the impact rating.	
David Rivera - New York Power Authority - 3	

Answer	No
Document Name	
Comment	
The language of several Reference Models states “When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary.” This language sounds like a Requirement. Recommend striking this sentence in all locations because the diagrams should be illustrative, allowing the Responsible Entity Flexiblity to implement appropriate security controls, as provided by the Requirements language. Also recommend striking the final sentence in Reference Models 1, 2 and 3. These security ocntrols are good suggestions and could be added as suggestions at the beginning of the Guidelines and Technical Basis.	
Likes 0	
Dislikes 0	
Response	
The SDT agrees that this should be made as an example and not a requirement for a particular type of access control. The G&TB has been changed accordingly.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Comment 1: *Language provided in Reference Model 10 contains substantive impact on how entities identify traffic as routable: "In similar configurations, the Responsible Entity should closely evaluate the transport entering or leaving the asset containing low impact BES Cyber System(s). If the communication entering or leaving the asset containing low impact BES Cyber System(s) was routable (such as serial*	

encapsulated in TCP/IP or UDP/IP as depicted Reference Model 2 or Reference Model 5), then the criteria requiring electronic access controls would be met."

Specifically, when utilizing communications circuits from a third party communications provider, an entity has no control or knowledge over the transport level technologies employed. From an entity's perspective, a 56K four-wire circuit is completely non-routable. However, the telecom provider may convert it to IP based communications in the telecom transport pathway prior to converting it back to a 56K four-wire circuit when entering a remote facility.

These transport-layer characteristics are transparent to the devices at each end of a communications link. The criteria specified in Reference Model 10 implies that potential encapsulations and conversions, outside of an entity's control (or even awareness), may qualify an otherwise non-routable communications link as routable.

As written, to verify transport level characteristics as provided in Reference Model 10 would require auditing all transport layer equipment and configurations as employed by the telecom provider.

TVA suggests that specific technical criteria that qualifies traffic as routable be included in a NERC Glossary term instead of language contained in a "Supplemental Material" section of a standard.

Comment 2:

Language provided in the section headed "Insufficient Access Controls" contains substantive impact on communication options available for use by entities: "Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include: […] A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan."

As written, the last sentence prevents the use of all internet based communications solutions that utilize a public IP address. This includes any cellular, satellite, or ISP based service. Many acceptable, and secure, internet based communications solutions exist where data can be appropriately secured. Most of these solutions would utilize some form of VPN or SSL technology. Access control is not contingent upon what IP addresses may or may not be used.

TVA recommends striking this bullet completely or clarifying the language to accommodate secure internet based communication solutions.

Likes 0	
Dislikes 0	
Response	
The SDT acknowledges the concern and has updated the reference model to refer to the transport as “protocol independent transport” to clarify that assessment of the internal technology leveraged in carrier networks is not intended. The standard does not preclude the use of a public IP address, provided there are effective electronic access controls implemented to meet the security objective of the requirement	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
The previous version of CIP-003-7 presented examples of asset boundaries and explicitly allowed extended asset boundaries beyond the property line. In order to prevent the addition of communications control equipment without significant gain in security, we believe that the SDT should explicitly extend the asset limits provided that physical or electronic controls are in place. The diagrams should reflect this option.	
Likes 0	
Dislikes 0	
Response	
The requirement is plan-based which allows the entity to determine what is inside and outside the asset, and subsequently implement the appropriate access control(s) that provide a sufficient level of protection to each low impact BCS contained within the asset(s). Although CIP-002 provides for the distinct identification of the asset(s) containing low impact BES Cyber System(s), there is no part of CIP-003 that precludes the entity from utilizing the same physical and electronic access controls for asset(s) at the same location. If implemented properly, this will not change the impact rating of the BES Cyber System(s). However, entities should be cautious not to create a shared BES Cyber System, which could affect the impact rating.	

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA generally agrees with the Guidelines and Technical Basis section, but sees two items that need addressing. While the SDT acknowledged there are concerns regarding shared facilities, FMPA does not believe the revised language completely addresses those concerns. Section 2 of Attachment 1 still states "**[e]ach** Responsible Entity shall control physical access." This simply does not work at share facilities because more than one entity cannot have control at the same time. It is essential for entities with BES Cyber Systems in shared facilities to be able to enter into agreements that identify the Repsonsible Entity controlling physical access. FMPA supports Seminole Electric Cooperative, Inc.'s proposed language for addressing shared facilities. Also, Reference Models 3 and 7 use the term "Non BES Cyber System" while others use the term "Non-BES Cyber Asset". FMPA believes cyber assest more accurately reflects what these devices are and that all the models should use consistent language.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, but this is outside of the scope of this posted revision.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	

Comment
N&ST recommends updating this section to reflect N&ST-recommended revised definition of LERC. Comments on specific reference models: N&ST believes Reference Model 6 (“Indirect Access”) is problematic in several regards. First of all, having attempted to respond to FERC’s directive to clarify what is meant by “direct” access by simply eliminating the word from CIP-003, the SDT reopens the debate by introducing the concept of “*indirect* access.” Second, N&ST believes the Reference Model’s assertion that the depicted “indirect access” “...meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset...” is incorrect if the depicted non-BES Cyber Asset is terminating the routable protocol connection between the “external” Cyber Asset and itself. N&ST recommends either eliminating this example or revising it to indicate there is *not* communication between the low impact BES Cyber System and an “external” Cyber Asset if the non-BES Cyber Asset inside the asset is providing an application-layer protocol break. If N&ST's proposed revised definition of LERC was applied to this Reference Model, N&ST believes LERC would not be present in this case. Reference Model 5 (“User Authentication”) has similar problems. Is the depicted non-BES Cyber Asset that is performing authentication continuing the same communications session from the external Cyber Asset to the low impact BES Cyber System by performing IP to serial protocol conversion, such as depicted in Reference Model 2? If so, N&ST agrees that there is communication between the low impact BES Cyber System and the external Cyber Asset. If, on the other hand, (1) the authenticating non-BES Cyber Asset is terminating the routable protocol connection from outside the asset and, (2) a user, once authenticated by that Cyber Asset, must initiate a new, serial communications session between the authenticating non-BES Cyber Asset and the low impact BES Cyber System, then N&ST believes the proposed electronic access control requirement would not be applicable. If N&ST's proposed revised definition of LERC was applied to this Reference Model, N&ST believes LERC would not be present in this case.
Likes 0	
Dislikes 0	
Response
Because there is communication from a Cyber Asset outside destined for the low impact BES Cyber System inside the asset through the non-BES Cyber Asset, there needs to be electronic access controls. As depicted in this Reference Model, one approach to doing this is the

designation of the security device as the electronic access control. Depending on the configuration of the non-BES Cyber Asset, it could also be used as the required electronic access control.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST recommends updating this section to reflect N&ST-recommended revised definition of LERC. Comments on specific reference models: N&ST believes Reference Model 6 (“Indirect Access”) is problematic in several regards. First of all, having attempted to respond to FERC’s directive to clarify what is meant by “direct” access by simply eliminating the word from CIP-003, the SDT reopens the debate by introducing the concept of “*indirect* access.” Second, N&ST believes the Reference Model’s assertion that the depicted “indirect access” “...meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset...” is incorrect if the depicted non-BES Cyber Asset is terminating the routable protocol connection between the “external” Cyber Asset and itself. N&ST recommends either eliminating this example or revising it to indicate there is *not* communication between the low impact BES Cyber System and an “external” Cyber Asset if the non-BES Cyber Asset inside the asset is providing an application-layer protocol break. If N&ST's proposed revised definition of LERC was applied to this Reference Model, N&ST believes LERC would not be present in this case. Reference Model 5 (“User Authentication”) has similar problems. Is the depicted non-BES Cyber Asset that is performing authentication continuing the same communications session from the external Cyber Asset to the low impact BES Cyber System by performing IP to serial protocol conversion, such as depicted in Reference Model 2? If so, N&ST agrees that there is communication between the low impact BES Cyber System and the external Cyber Asset. If, on the other hand, (1) the authenticating non-BES Cyber Asset is terminating the routable protocol connection from outside the asset and, (2) a user, once authenticated by that Cyber Asset, must initiate a new, serial communications session between the authenticating non-BES Cyber Asset and the low impact BES Cyber System, then N&ST believes the proposed electronic access control requirement would not be applicable. If N&ST's proposed revised definition of LERC was applied to this Reference Model, N&ST believes LERC would not be present in this case.	
Likes 0	

Dislikes 0	
Response	
Because there is communication from a Cyber Asset destined for the low impact BES Cyber System inside the asset containing, there needs to be an electronic access control. As depicted in this Reference Model, one approach to doing this is the implementation of a non-BES Cyber Asset to perform authentication, therefore providing electronic access controls.	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
This section needs to be modified to be congruent with a LERC definition which is allows for the exception of traffic not destined for a local BES cyber system. This section includes a diagrams which need modified as well. None of the reference models depict traffic crossing the asset boundary but are destined for other sites and therein lies the problem with the definition being so all inclusive.	
Likes 0	
Dislikes 0	
Response	
The SDT appreciates your comment. Please see the SDT's response to your comment in question 1.	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	

The language of Reference Models 1, 2 and 3 states “When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary.” MMWEC recommends striking this sentence because it contradicts Section 3 in Attachment 1 and Attachment 2, which allow flexibility in how the Responsible Entity chooses to implement access controls.	
Likes 0	
Dislikes 0	
Response	
The SDT agrees that this should be made as an example and not a requirement for a particular type of access control. The G&TB has been changed accordingly.	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	No
Document Name	
Comment	
The conceptual diagrams continue to appear confusing at best. We have concerns about how the GTB are factored into Compliance and Enforcement. In some cases it appears that they create “requirements” that must be incorporated into your program; this is inconsistent with prior FERC precedent. On the other hand, it is not clear whether or not you can rely on the GTB in developing your program and ensuring compliance.	
Likes 0	
Dislikes 0	
Response	
The SDT develops the GTB to convey the intent of the requirement language and capture the development concepts. The ERO endorsement of the GTB is outside of the SDT development process.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion	

Answer	No
Document Name	
Comment	
The language of several Reference Models states “When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary.” This language sounds like a Requirement. Recommend striking this sentence in all locations because the diagrams should be illustrative, allowing the Responsible Entity Flexiblity to implement appropriate security controls, as provided by the Requirements language. Also recommend striking the final sentence in Reference Models 1, 2 and 3. These security ocntrols are good suggestions and could be added as suggestions at the beginning of the Guidelines and Technical Basis.	
Likes 0	
Dislikes 0	
Response	
The SDT agrees that this should be made as an example and not a requirement for a particular type of access control. The G&TB has been changed accordingly.	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
We do not support the Guidelines nor Technical Basis as we do not support the language in this draft Standard.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment.	
Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
1) A Responsible Entity should be able to develop their own approach based on their unique electronic access control implementation methodology. 2) The technical controls are helpful guidance, but the requirements should not require a list of low impact BES Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
The SDT agrees that this should be made as an example and not a requirement for a particular type of access control. The G&TB has been changed accordingly. This a plan approach requirement. However, a list of low impact BES Cyber Systems is not required under CIP-002. The SDT suggests that Responsible Entities review the G&TB, the RSAW, and corresponding measure(s) for additional information.	
Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC	
Answer	No
Document Name	
Comment	
Under the Dial-up Connectivity section, Reclamation recommends the first paragraph be changed to:	

"Dial-up Connectivity to a low impact BES Cyber System may be authenticated using one or more of the following access control methods: 1. The modem allowing access to a low impact BES Cyber System is configured to dial out only (no auto-answer) to a preprogrammed number to deliver data, 2. The modem allowing access to a low impact BES Cyber System is configured as a dialback modem, 3. The modem allowing access to a low impact BES Cyber System is enabled or powered up by on-site personnel only when needed, and disabled when not in use. 4. The modem allowing access to a low impact BES Cyber System is enabled or powered up remotely from a Control Center or control room only when needed, and disabled when not in use. 5. The modem allowing access to a low impact BES Cyber System is configured for auto-answer, but the communications are encrypted, protecting Cyber Assets from unauthorized control within the low impact BES Cyber System. 6. The low impact BES Cyber System is configured with access control when accessed using Dial-up Connectivity."

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment but declines to make the proposed changes.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standards Review Group requests consideration of further refinement to the language of the GTB in Requirements R1 and R2.	

Specific to Requirement 1, the language is not consistent with the GTB reference section to R1. Specific to Requirement 2, it is unclear which document Attachment 1 is associated with (CIP-002 or CIP-003-7).	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment; however, the comment does not provide sufficient detail to make modifications. The SDT thanks you for your comment but declines to make further modifications. Unless otherwise stated, the attachment refers to the standard in which it is contained.	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes the technical diversity of the examples provide sufficient guidance for consistent interpretation and application of the standard.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your encouraging comment.	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	

While Seminole supports the technical merits and the Guidelines and Technical Basis changes, Seminole refers the team to additional issues identified in question 7 that may best be addressed in the Guidelines and Technical Basis section of the standard.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, but this is outside of the scope of this posted revision.	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the content, however recommends that the requirement language be reviewed against the diagrams provided to ensure that there is not ambiguity or confusion created between the two portions of the standard. While we believe the current language is an improvement, AZPS may not be able to vote affirmatively on this requirement if the ambiguity is not addressed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The diagrams have been reviewed and any updates made in response to industry comments.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Seattle in particular appreciates the addition of Reference Model 10, to illustrate the common case of a SONET system carrying both routable and non-routable traffic.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your encouraging comment.	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP appreciates the use of example diagrams. Reference model 10 is particularly useful. However, MPLS is still not addressed within the diagrams. SRP requests the SDT create an example diagram to address MPLS as the transport network. Would only the out of band management network be considered as the electronic access or is it expected the MPLS transport connection must traverse an electronic access control such as a firewall?	
Likes 0	
Dislikes 0	
Response	
The SDT agrees and will change the diagram to "protocol independent transport" so that current and future transport protocols are included.	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	

Comment
Under the draft, electronic access controls must be implemented for routable connections to low impact BES Cyber Systems such that only “necessary” traffic is permitted. The determination of what is “necessary” remains in the hands of the Responsible Entity, but documentation to support why communications are “necessary” would likely be required because these determinations will need to be justified. Documenting why the permitted traffic for each routable connection is “necessary” could be extremely burdensome. The GTB should explicitly allow Responsible Entities to define the necessary communications generically, so that separate documentation need not be maintained for each routable communication at each site. Propose that the GTB specifically state that the intent is not to require access control list or other line by line justifications.

Likes 0	
Dislikes 0	

Response
Requirement R2 is a plan-based requirement, and evidence to demonstrate compliance is based on content in its plan. The SDT suggests that Responsible Entities review the G&TB, the RSAW, and corresponding measure(s) for additional information.

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment
We believe that “the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level.” However, we are concerned with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says “the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process.” We also understand that at the November MRC meeting NERC Staff and the Standards Committee leadership agreed to work together on a way forward on the GTB that affords deference. EEI encourages NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.

Likes 1	Massachusetts Municipal Wholesale Electric Company, 5, Gordon David
Dislikes 0	
Response	
The SDT develops the GTB to convey the intent of the requirement language and capture the development concepts. The ERO endorsement of the GTB is outside of the SDT development process.	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	Yes
Document Name	
Comment	
PSEG agrees with the EEI comments.	
Likes 0	
Dislikes 0	
Response	
We believe that "the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level." However, we are concerned with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says "the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process." We also understand that at the November MRC meeting NERC Staff and the Standards Committee leadership agreed to work together on a way forward on the GTB that affords deference. EEI encourages NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	

We align with Edison Electric Institute's (EEI) comments, stating:

We believe that "the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level." However, we are concerned with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says "the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process." We also understand that at the November MRC meeting NERC Staff and the Standards Committee leadership agreed to work together on a way forward on the GTB that affords deference. EEI encourages NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.

Likes 0	
Dislikes 0	

Response

We believe that "the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level." However, we are concerned with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says "the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process." We also understand that at the November MRC meeting NERC Staff and the Standards Committee leadership agreed to work together on a way forward on the GTB that affords deference. EEI encourages NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

We align with Edison Electric Institute's (EEI) comments, stating:

We believe that "the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level." However, we are concerned with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says "the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process." We also understand that at the November MRC meeting NERC Staff and the Standards Committee leadership agreed to work together on a way forward on the GTB that affords deference. EEI encourages NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.	
Likes 0	
Dislikes 0	
Response	
We believe that "the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level." However, we are concerned with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says "the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process." We also understand that at the November MRC meeting NERC Staff and the Standards Committee leadership agreed to work together on a way forward on the GTB that affords deference. EEI encourages NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Tri-State appreciates the SDT's work on the Reference Models; however, we recommend the SDT split up the three concepts displayed in Model 8. The current diagram is a bit confusing and may be misinterpreted as one combined concept, rather than three separate ones. Tri-State would appreciate the inclusion of some examples of what equipment or configurations might qualify as a "Uni-directional Gateway". There has been a lack of consistency among regions as to what devices would apply for this designation and we would like	

some clarity from the SDT on this. Specifically, we wonder whether the SDT considers a properly configured firewall to be included as a part of this designation?	
Likes 0	
Dislikes 0	
Response	
The SDT appreciates the concerns but asserts that model 8 provides a valuable example of how multiple concepts may come together to provide effective electronic access controls. The SDT thanks you for your comments and notes that a firewall does not qualify as a uni-directional gateway but may be used in conjunction with a uni-directional gateway to provide electronic access controls.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees that "the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level." However, Southern Company joins EEI in expressing concern with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says "the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process." Southern Company joins EEI to encourage NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable. Page 42 of 65, Reference Model 3: "The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be another asset containing low impact BES Cyber System(s)." **SOCO Comment:** It appears this statement should read "… that may or may not be ***at*** another asset containing low impact BES Cyber System(s)." The word *"at"* appears to be missing in this statement.	

Page 42 of 65, Reference Model 3: "Care should be taken that electronic access to or between each asset is through the electronic access controls at the centralized location." **SOCO Comment:** Consider the following edits to this statement: "Care should be taken that electronic access to or between each asset is through the ***Cyber Asset(s) determined by the Responsible Entity to be performing/providing*** electronic access controls at the centralized location." Page 43 of 65, Reference Model 4: Was the term "bi-directional" intentionally struck from the requirement language? This seems to cause issues in Reference Model 4 – Uni-directional Gateway. As the modifications to the Standard are read now, inbound **OR** outbound communications to assets containing Low Impact BES Cyber Systems require protections; Section 3, 3.1 Part ii – "using a routable protocol when entering **OR** leaving the asset." Therefore, the uni-directional gateway allowing routable communications only to flow outside of the asset containing Lows would still require protections.

Likes 0	
Dislikes 0	

Response
-The SDT develops the GTB to convey the intent of the requirement language and capture the development concepts. The ERO endorsement of the GTB is outside of the SDT development process. - The SDT thanks you for your comment and has made the recommended modifications. -The SDT asserts that controls which enforce one-way communications are themselves among the electronic access controls that should be implemented in a manner to meet the security objective outlined in Attachment 1, Section 3.

Michael Mertz - PNM Resources - 3	
Answer	Yes
Document Name	
Comment	

We believe that “the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level.” However, we are concerned with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says “the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process.” We also understand that at the November MRC meeting NERC Staff and the Standards Committee leadership agreed to work together on a way forward on the GTB that affords deference. EEI encourages NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.	
Likes 0	
Dislikes 0	
Response	
The SDT developed the GTB to convey the intent of the requirement language and capture the development concepts. The ERO endorsement of the GTB is outside of the SDT development process.	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Malozewski - Hydro One Networks, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael DeLoach - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rich Hydzik - Rich Hydzik On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Rich Hydzik	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alexander Vedvik - Public Service Commission of Wisconsin - 9	
Answer	
Document Name	
Comment	

The PSCW abstains. However, we recommend NERC consider comments by registered entities impacted by this standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's response to #1.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's response in Question 1.	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	
Document Name	
Comment	
adopt PSEG comments	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment.	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	
Document Name	
Comment	
We believe that “the GTB provides support for the technical merit of the requirement [R2] and provides example diagrams that illustrate various electronic access controls at a conceptual level.” However, we are concerned with the impact that the recent Guidelines and Technical Basis Disclaimer (shared with the Standards Committee on 10/19/16) may have on the use of the GTB. In particular, the sentence that says “the ERO neither endorses nor approves the Supplemental Material as part of the Reliability Standards development process.” We also understand that at the November MRC meeting NERC Staff and the Standards Committee leadership agreed to work together on a way forward on the GTB that affords deference. EEI encourages NERC and the Standards Committee leadership to work to provide GTB deference as soon as practicable.	
Likes 0	
Dislikes 0	
Response	
The SDT developed the GTB to convey the intent of the requirement language and capture the development concepts. The ERO endorsement of the GTB is outside of the SDT development process.	

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) date for the revisions made to CIP-003, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer, please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.	
Michael Mertz - PNM Resources - 3	
Answer	No
Document Name	
Comment	
The CIP-003-6 plan for Requirement R1, part 1.2 is due April 1, 2017, which depends on the use of LERC and LEAP, which the Commission has ordered NERC to modify.The CIP-003-7 modifications remove the use of LERC and LEAP terms. Although we agree with the modifications, we do not believe that these modifications can be made and approved by the Commission by this date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the Commission approves the modifications. We urge that NERC and FERC consider this implementation impact on Requirement R1 and recommend that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan. Regarding R1, part 1.2, the SDT acknowledges the concern; however, the development schedule of the SDT does not enable the	

ability to request a change to the approved Implementation Plan prior to its enforcement date. This issue has been presented to NERC staff for their consideration.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standards Review Group requests delaying the specification of an effective date until the SDT has resolved any issues within the standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan. Regarding conflicting issue areas, the SDT appreciates your concern. However, the SDT is obligated to meet the March 31, 2017 FERC deadline for LERC and has received significant comment from industry requesting that a minimum number of versions be drafted to allow entities to have a complete set of revised requirements as soon as possible to reduce impact. Meeting both objectives has led to overlap in the posting schedule.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Although Southern Company agrees with the proposed modifications, as noted by EEI, Southern Company does not find that these modifications can be made and approved by the Commission by the required date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the Commission approves the modifications. Southern Company joins EEI in urging that NERC and FERC consider this implementation impact on Requirement R1 and	

recommends that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan. Regarding R1, part 1.2, the SDT acknowledges the concern; however, the development schedule of the SDT does not enable the ability to request a change to the approved Implementation Plan prior to its enforcement date. This issue has been presented to NERC staff for their consideration.	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	No
Document Name	
Comment	
The CIP-003-6 plan for Requirement R1, part 1.2 is due April 1, 2017, which depends on the use of LERC and LEAP, which the Commission has ordered NERC to modify. The CIP-003-7 modifications remove the use of LERC and LEAP terms. Although we agree with the modifications, we do not believe that these modifications can be made and approved by the Commission by this date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the Commission approves the modifications. We urge that NERC and FERC consider this implementation impact on Requirement R1 and recommend that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan. Regarding R1, part 1.2, the SDT acknowledges the concern; however, the development schedule of the SDT does not enable the ability to request a change to the approved Implementation Plan prior to its enforcement date. This issue has been presented to NERC staff for their consideration.	
Rich Hydzik - Rich Hydzik On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Rich Hydzik	
Answer	No
Document Name	
Comment	
The CIP-003-6 plan for Requirement R1, part 1.2 is due April 1, 2017, which depends on the use of LERC and LEAP, which the Commission has ordered NERC to modify. The CIP-003-7 modifications remove the use of LERC and LEAP terms. Although we agree with the modifications, we do not believe that these modifications can be made and approved by the Commission by this date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the Commission approves the modifications. We urge that NERC and FERC consider this implementation impact on Requirement R1 and recommend that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan. Regarding R1, part 1.2, the SDT acknowledges the concern; however, the development schedule of the SDT does not enable the ability to request a change to the approved Implementation Plan prior to its enforcement date. This issue has been presented to NERC staff for their consideration.	
Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC	
Answer	No
Document Name	

Comment	
Reclamation recommends a more achievable implementation plan of 24 months from the date of FERC approval.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
1) The implementation plan should not occur until 2019. We do not support the proposed target date of September 1, 2018, because there are several other requirements that already will go into effect on this date. The burden of compliance with this proposal would add significant resources and costs with implementing these low impact security measures, especially for smaller entities. 2) The implementation plan should allow for an additional budgeting cycle to ensure industry has time to implement such controls.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Michael DeLoach - AEP - 3	

Answer	No
Document Name	
Comment	
Twelve months is insufficient time to react to the extremely large number of assets containing low impact BES Cyber Systems. AEP has almost 2000. This is only the first of several potential revisions to CIP-003 necessary to completely address FERC Order 829??. Two years is probably needed to fully comply with this the first of several revisions CIP-003. The hope is that twelve months will accommodate all the revisions of CIP-003 resulting from the Order. This is consistant with the original allowance in the CIP-003-5 implementation plan that was approved. Lets do it once.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	
Due to budget cycles and quantity of equipment that must be installed, we propose keeping the language included in the “General Consideration” section but extend the interval from 12 months to 18 months.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame	
Answer	No
Document Name	
Comment	
1. The implementation plan should not occur until 2019. We do not support the proposed target date of September 1, 2018, because there are several other requirements that already will go into effect on this date. The burden of compliance with this proposal would add significant resources and costs with implementing these low impact security measures, especially for smaller entities. 2. The implementation plan should allow for an additional budgeting cycle to ensure industry has time to implement such controls.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	No
Document Name	
Comment	

While we appreciate the increase of over 9 months included in the original posting, we believe that 12 months is insufficient for the successful implementation of these requirements. Through the inclusion of indirect communications now being required to meet the security objective of implementing electronic access controls that permit only necessary inbound and outbound access, the SDT has substantially increased the evidentiary burden to document the controls implemented for this use case. Given the large volume of assets at low impact, 12 months is not long enough to properly implement this revised control.

We understand that the SDT has extended its planned implementation plan for Transient Cyber Assets at low impact to 18 months and believe that the implementation timeline for the LERC requirements should also be adjusted to 18 months. This will allow sufficient time for LERC implementation and allow for operational efficiencies to occur by implementing the LERC requirements and the TCA requirements concurrently.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

We align with Edison Electric Institute's (EEI) comments, stating:

The CIP-003-6 plan for Requirement R1, part 1.2 is due April 1, 2017, which depends on the use of LERC and LEAP, which the Commission has ordered NERC to modify. The CIP-003-7 modifications remove the use of LERC and LEAP terms. Although we agree with the modifications, we do not believe that these modifications can be made and approved by the Commission by this date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the Commission approves the modifications. We urge that NERC and FERC consider this implementation impact on Requirement R1 and

recommend that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan. Regarding R1, part 1.2, the SDT acknowledges the concern; however, the development schedule of the SDT does not enable the ability to request a change to the approved Implementation Plan prior to its enforcement date. This issue has been presented to NERC staff for their consideration.	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	
See EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan. Regarding R1, part 1.2, the SDT acknowledges the concern; however, the development schedule of the SDT does not enable the ability to request a change to the approved Implementation Plan prior to its enforcement date. This issue has been presented to NERC staff for their consideration.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No

Document Name	
Comment	
Comments: We align with Edison Electric Institute's (EEI) comments, stating: *The CIP-003-6 plan for Requirement R1, part 1.2 is due April 1, 2017, which depends on the use of LERC and LEAP, which the Commission has ordered NERC to modify. The CIP-003-7 modifications remove the use of LERC and LEAP terms. Although we agree with the modifications, we do not believe that these modifications can be made and approved by the Commission by this date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the Commission approves the modifications. We urge that NERC and FERC consider this implementation impact on Requirement R1 and recommend that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan. Regarding R1, part 1.2, the SDT acknowledges the concern; however, the development schedule of the SDT does not enable the ability to request a change to the approved Implementation Plan prior to its enforcement date. This issue has been presented to NERC staff for their consideration.	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
We suggest extending the proposed implementation time-period for electronic and physical access controls by revising the wording to: "later of April 1, 2019 or the first day of .....". The transition to CIP Version 5/6 utilized significant entity resources during the past two	

years. Given that Low Impact BES Cyber Systems pose a lower risk to system reliability (by definition), we submit that allowing additional time is reasonable and would allow entities time to better integrate this work with other priorities.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Revising standards and then expecting the industry to change directions and then comply with the requirements in the same amount of time is not a feasible approach. Although the depth of requirements associated with Low Impact BCS is less compared to the High and Medium BCS the breadth of what it will encompass is much greater. Entities have had to halt or slow the progress on their approach considering the changes to LERC, which is a major component to CIP-003. As these sections of CIP-003 had a later implementation due to their newness and scope and now there are major changes to how they will be approached there is no reason why the implementation schedule can't be moved by at least 6 to 12 months which will be the amount of time from when the standards went into effect (7/1/2016) and when FERC will hopefully approves them (2nd or 3rd Qtr of 2017.) I would propose the implementation date be the later of either April 1, 2019 or July 1 ,2019 or 12 months from the date of approval.	
Likes 0	
Dislikes 0	
Response	
The SDT agrees with your comment regarding the need for additional time to implement the revised requirements and has extended the implementation plan to 18 months following regulatory approval.SDT	

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA appreciates the efforts of the SDT to address the comments from the previous draft. However, we believe that 12 months is not an adequate amount of time to complete the implementation of these revised requirements. Through the inclusion of indirect communications now being required to meet the security objective of implementing electronic access controls that permit only necessary inbound and outbound access, the SDT has substantially increased the evidentiary burden to document the controls implemented for this use case. Given the large volume of assets at low impact, 12 months is not long enough to properly implement this revised control. We understand that the SDT has extended its planned implementation plan for Transient Cyber Assets at low impact to 18 months and believe that the implementation timeline for the LERC requirements should also be adjusted to 18 months. This will allow sufficient time for LERC implementation and allow for operational efficiencies to occur by implementing the LERC requirements and the TCA requirements concurrently.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	No
Document Name	
Comment	
PSEG agrees with the EEI comments.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Ronnie Frizzell - Arkansas Electric Cooperative Corporation - 4	
Answer	No
Document Name	
Comment	
I agree with the comments from NRECA	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The CIP-003-6 plan for Requirement R1, part 1.2 is due April 1, 2017, which depends on the use of LERC and LEAP, which the Commission has ordered NERC to modify. The CIP-003-7 modifications remove the use of the LERC and LEAP terms. Although we agree with the modifications, we do not believe that these modifications can be made and approved by the Commission by this date, which will require Responsible Entities to comply with two versions of CIP-003 – first by April 1, 2017 for R1, part 1.2 and then a second, version 7, once the	

Commission approves the modifications. We urge that NERC and FERC consider this implementation impact on Requirement R1 and recommend that the SDT consider replacing the effective date of Requirement R1, part 1.2, subpart 1.2.3 with the effective date of CIP-003-7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan. Regarding R1, part 1.2, the SDT acknowledges the concern; however, the development schedule of the SDT does not enable the ability to request a change to the approved Implementation Plan prior to its enforcement date. This issue has been presented to NERC staff for their consideration.	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Due to budget cycles and quantity of equipment that must be installed, we propose keeping the language included in the “General Consideration” section but extend the interval from 12 months to 18 months.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No

Document Name	
Comment	
The CIP requirements for low impact BES Cyber Systems are currently in flux and entities will not have certainty regarding low impact requirements until they are approved by the Commission. In addition, the sheer number of assets containing low impact BES Cyber Systems is substantial. It will take entities time to implement proper physical and electronic access controls at all the various locations. CenterPoint Energy believes it is reasonable to request additional time to implement the requirements given that the facilities are low risk to the reliability of the BES. CenterPoint Energy recommends the effective date for CIP-003-7 revisions to be delayed 18 months after FERC approval. Additionally, CenterPoint Energy agrees with EEI's comments to align the implementation date of CIP-003-6 R1, Part 1.2.2 and 1.2.3 (cyber security policies) with the effective date of the LERC changes to Attachment 1, Section 2 and Section 3 (cyber security plans). Although CenterPoint Energy supports the retirement of the LERC/LEAP terms in CIP-003-7, the LERC/LEAP terms are still used in the currently approved CIP-003-6 requirements that are effective April 1, 2017. Therefore, entities will need to comply with two versions of the CIP-003 standard between April 1, 2017 and the effective date of version 7. This could cause entities substantial rework and resource constraints because what is being implemented is a moving target. It will be more efficient and effective for entities to implement one version of the standard and align their cyber security policies with the cyber security plans for requirement CIP-003-7, Attachment 1, Section 2 and Section 3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan. Regarding R1, part 1.2, the SDT acknowledges the concern; however, the development schedule of the SDT does not enable the ability to request a change to the approved Implementation Plan prior to its enforcement date. This issue has been presented to NERC staff for their consideration.	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	No

Document Name	
Comment	
AECC supports the comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Process development and implementation of Low BCS electronic access controls has been significantly delayed and remains contingent upon requirements finalization. Propose allowance of a minimum of 24 months from FERC approval date to compliance date for CIP-003-7 R2, Attachment 1 Sections 2 and 3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
David Rivera - New York Power Authority - 3	
Answer	No

Document Name	
Comment	
Due to budget cycles and quantity of equipment that must be installed, we propose keeping the language included in the “General Consideration” section but extend the interval from 12 months to 18 months.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	

For the implementation plan which is 12 months, Dominion recommends an 18 month implementation period for the following reasons:

- Time is needed for entities to assess and confirm indirect access as an acceptable access control.
- New environments may be in scope.
- While this revision approach is more consistent with the currently approved CIP version6 requirements, the revisions necessitate that entities conduct an impact assessment to determine what changes the revisions create and what is currently in place from the assesments performed for CIP version 6 implementation.
- Revision iterations always require some time to assess and verify points of change.

Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan.	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	Yes
Document Name	
Comment	

Did the SDT intend to modify the enforceability of CIP-003-6 via this Implementation Plan? If so, FMPA recommends the addition in bold to the language below. "The Responsible Entity shall not be required to include in its cyber security plan(s) elements related to Sections 2 and 3 of **CIP-003-6** Attachment 1 until the effective date of CIP-003-7."	
Likes 0	
Dislikes 0	
Response	
The SDT acknowledges the concern; however, the development schedule of the SDT does not enable the ability to request a change to the approved Implementation Plan prior to its enforcement date. This issue has been presented to NERC staff for their consideration.	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	

Comment	
Procurement, design, installation, and configuration of electronic access controls.	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA supports this timeline. Site inventories and the work to develop scope for new programs to meet the standard requirements will require time to approve, develop and implement a sustainable compliance program.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

OPG is in the process of surveying all of its Low Impact Rating BES assets to determine where there is communication between the asset or a Low Impact BES Cyber Asset within the asset with an external Cyber Asset. If the communication is using a routable protocol then the appropriate electronic security controls are being selected and installed to permit only neccessary inbound and outbound electronic access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Yuguang Xiao - Manitoba Hydro - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Blair Mukanik - Manitoba Hydro - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	
Document Name	
Comment	
adopt PSEG comments	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE respectfully requests the SDT provide a basis for its decision to adopt a 12-month compliance window, including any data it considered in determining that this was an appropriate window for affected entities to meet their compliance obligations under the revised Standards. Texas RE requests the revised implementation plan clarify Section 4, 4.5; the testing the Cyber Security Incident response plan(s). There is confusion amongst the Industry on whether the plan must be tested on or before April 1, 2017, or 36 calendar months after the effective date.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that additional time may be required and has proposed changes to the implementation plan. Regarding the first occurrence comment, although the SDT acknowledges the concern, it is outside of the scope of this industry-approved SAR. This issue has been presented to NERC staff for their consideration.	
Alexander Vedvik - Public Service Commission of Wisconsin - 9	
Answer	
Document Name	
Comment	
The PSCW abstains.	
Likes 0	
Dislikes 0	
Response	

7. If you have additional comments on the proposed revisions to address the FERC directive regarding the LERC definition that you have not provided in response to the questions above, please provide them here.	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
Thank you for retiring this definition.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	
Document Name	
Comment	
ITC Holdings does not agree with changing the 'Guidelines and Technical Basis' (GTB) document to 'Supplemental Material'. Changing the name of the document does not solve any of the issues regarding whether or not regions will uphold it – it only causes more confusion. The ballot body approves the GTB as part of the standard and it should be agreed to by all regions to ensure there is consistency in how the GTB is treated.	
Likes 0	

Dislikes 0	
Response	
The SDT does not have the flexibility to modify the NERC template, which defines the section name. The Guidelines and Technical Basis will continue to be a section within "Supplemental Material".	
Jeff Johnson - Sempra - San Diego Gas and Electric - 4 - WECC	
Answer	
Document Name	
Comment	
No comments at this time.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	
Document Name	
Comment	
Dominion requests that NERC petition FERC to delay and/or cancel CIP-003-6 (in a similar manner to version 4) until the currently approved CIP version is superseded by CIP version 7. Requiring Registered Entities to identify and document LERCs and LEAPs only to remove those requirements is an unreasonable burden and does not contribute to the reliable operation of the BES.	
Likes 0	
Dislikes 0	

Response
Although the SDT acknowledges the concern, it is outside of the scope of work of the SDT.

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	
Document Name	
Comment	

Seminole appreciates the Standard Development Team's work on this requirement, especially the efforts to make this a non-prescriptive risk based security standard. While Seminole currently supports the Guidelines and Technical Basis section related to the diagrams, there are additional issues to address and, therefore, Seminole is voting no on the current ballot.

The term asset is an undefined term. This term is a core component of the requirement. Without a definition or guidance within the document clarifying the intent of the term asset, it is likely that in certain cases audit teams and entities will interpret this term differently. Elimination of the phrase asset boundary reduces but does not eliminate this concern. The term asset should be addressed with a section in the Guidelines and Technical Basis. For example, It should be clarified whether the term asset refers to the entire location, the components within the location that contains a BES Cyber System, or to Cyber Assets and other Facilities, systems, and equipment within that location "owned by each Responsible Entity in Section 4.1" (CIP-003 section 4.2- Applicability). However, any changes should be carefully considered with respect to CIP-002-5.1.

Seminole continues to have concerns that assets with multiple entities having Cyber Assets in a single location is not adequately addressed. This is a particularly important topic in the FRCC region due to the high number of Transmission Operators that are interconnected in a small region. It is common that shared facilities such as substations with interconnections and substations owned by Distribution Providers to have multiple entities with Cyber Assets within a single control house. While the currently recommended approach is a Memorandum of Understanding, this approach leaves multiple entities at risk of a violation if the asset owner fails to provide appropriate physical security. Seminole recommends language similar to the following be placed in the Guidelines and Technical Basis section of the Standard to clarify the role of the Memorandum of Understanding:

"In cases where multiple entities have a Cyber Asset located that are protected in a common location and the security is provided by one entity, a signed and dated agreement such as a Memorandum of Understanding between the Cyber Asset(s) owner and the entity providing physical security sufficiently documents the specific party responsible for meeting physical security requirements."	
Likes 1	Gowder Chris On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins,
Dislikes 0	
Response	
The SDT thanks you for your support. The use of the term "asset" refers to assets identified as containing low impact BES Cyber System(s) pursuant to CIP-002. As described in the G&TB, the Responsible Entity has the flexibility to identify the electronic boundary surrounding the low impact BES Cyber System rather than using a physical boundary. With regards to assets with multiple entities having Cyber Assets in a single location, the SDT thanks you for your comment, but this is outside of the scope of this posted revision.	
David Rivera - New York Power Authority - 3	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	

Document Name	
Comment	
Seattle has one additional concern, that the approach to routable connectivity expressed in the present draft does not address the issue of mixed communications paths involving both routable and non-routable communications. As written, it appears that so long as a non-routable communications segment crosses the border of the BES asset containing the Low impact BES Cyber System, the entire system is judged to communicate non-routably. Although this is a simple and clear approach, it seems to conflict with the more nuanced approaches urged over the years since 2009 by FERC and regional regulators regarding the differentiation between external routable communications and non-routable communications. Seattle understands that another group from the CIP v7 SDT is developing a revised approach to External Routable Connectivity that considers the nuances of mixed communications modes. As such, Seattle is concerned that when that effort is complete, CIP-003-7 R2 Attachment 1 Item 3.1 will require revision (again) to reflect that change—and it will come after entities have implemented their communications controls for their Low assets. Seattle urges that the two efforts be aligned to minimize the chance of such a change and the attendant additional effort and expense that may be required to change, again, compliance programs, documentation, and actual field communication installations.	
Likes 0	
Dislikes 0	
Response	
The SDT developed the modifications for R2, Attachment 1 to provide additional clarity on when electronic access controls are required. While related, the paradigm for protections at low impact is distinct from that for medium and high impact. The SDT does not intend for its work at high and medium impact to require future modifications to the language it has currently drafted for low impact.	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	

Reference Model 8: The term “air gap” may not be universally understood and goes undefined in the standard. A pure reading of air gap is that there is no connectivity at all to the device. However, in a substation it is common to have contact oriented connected, while not serial or Ethernet, there is still a cable connected and therefore not a pure “air gap.” Exelon recommends replacing the use of “air gap” with “physical isolation from routable protocol” or using a red circle to depict no communication as in Reference Model 3 to be consistent with title and text of Reference Model 8.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. It is the SDT’s intention that the reference models be reviewed in context with the discussion included in the G&TB in which “air gap” is used and described.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
CenterPoint Energy is in favor of filing the TCA modifications and implementation plan with the LERC modifications, if possible.	
Likes 0	
Dislikes 0	
Response	
The SDT is working to provide a combined version to include the LERC and TCA modifications.	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	
Document Name	

Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	
Document Name	
Comment	
Based on our understanding from reading the requirements. Removing the terms LERC and LEAP doesn't remove the efforts required to implement and maintain low impact systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that substantial effort is required to effectively protect BES Cyber Systems regardless of the specific language used in NERC CIP Reliability Standards.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	

Comment
CIP Exceptional Circumstances has not been included within CIP-003-7 as drafted. CIP exceptional circumstances should be included as a provision for Low Impact Entities and therefore considered in this standard.

Likes 0	
Dislikes 0	

Response
The SDT will not be making this change under this posting. The CIP Exceptional Circumstance applicability will continue to be evaluated as the SDT continues to address the issue areas within the SAR.

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	

Comment
The intent of these revisions are understood and are an improvement for cyber security around BES Cyber Assets. Minnesota Power has concerns surrounding the lack of clarity as to how Registered Entities will comply with the Standard. The CIP Standards family has become more prescriptive over time (specifically the auditing approach by the Regional Entities), this Standard seems to be moving in a different direction, becoming less prescriptive and open. Though this approach is appreciated, NERC must provide clear guidance to the regional entities for auditing, in a consistent manner, to the Standard's intentions.

Likes 0	
Dislikes 0	

Response
The SDT continues to work with NERC on compliance measurement. This includes documenting the SDT intent within the Guidelines and Technical Basis, industry outreach, and consulting on the drafting of the RSAW.

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
The intent of these revisions are understood and are an improvement for cyber security around BES Cyber Assets. Minnesota Power has concerns surrounding the lack of clarity as to how Registered Entities will comply with the Standard. The CIP Standards family has become more prescriptive over time (specifically the auditing approach by the Regional Entities), this Standard seems to be moving in a different direction, becoming less prescriptive and open. Though this approach is appreciated, NERC must provide clear guidance to the regional entities for auditing, in a consistent manner, to the Standard's intentions.	
Likes 0	
Dislikes 0	
Response	
The SDT continues to work with NERC on compliance measurement. This includes documenting the SDT intent within the Guidelines and Technical Basis, industry outreach, and consulting on the drafting of the RSAW.	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	
Document Name	
Comment	
None at this time.	
Likes 0	
Dislikes 0	
Response	

Scott Brame - Scott Brame On Behalf of: doug white, North Carolina Electric Membership Corporation, 4, 3, 5; John Lemire, North Carolina Electric Membership Corporation, 4, 3, 5; Robert Beadle, North Carolina Electric Membership Corporation, 4, 3, 5; - Scott Brame	
Answer	
Document Name	
Comment	
We urge the SDT to stagger its posting schedule so different drafts of the CIP standards do not have overlapping deadlines to submit comments. Industry is currently focused on implementing the existing CIP V5 standards, while also paying attention to the development of these revisions. There should not be multiple deadlines assigned to this project, as this creates a strain on CIP subject matter experts to review and provide feedback on the proposed changes.	
Likes 0	
Dislikes 0	
Response	
The SDT appreciates your concern. However, the SDT is obligated to meet the March 31, 2017 FERC deadline for LERC and has received significant comment from industry requesting that a minimum number of versions be drafted to allow entities to have a complete set of revised requirements as soon as possible to reduce impact. Meeting both objectives has led to overlap in the posting schedule.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion	
Answer	
Document Name	
Comment	
None.	
Likes 0	

Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	
Document Name	
Comment	
no comments	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	
Document Name	
Comment	
adopt PSEG comments	
Likes 0	
Dislikes 0	
Response	
There were no PSEG comments submitted for this question.	

Colleen Campbell - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	
Document Name	
Comment	
We urge the SDT to stagger its posting schedule so different drafts of the CIP standards do not have overlapping deadlines to submit comments. Industry is currently focused on implementing the existing CIP V5 standards, while also paying attention to the development of these revisions. There should not be multiple deadlines assigned to this project, as this creates a strain on CIP subject matter experts to review and provide feedback on the proposed changes. We thank you for this opportunity to comment.	
Likes 0	
Dislikes 0	
Response	
The SDT appreciates your concern. However, the SDT is obligated to meet the March 31, 2017 FERC deadline for LERC and has received significant comment from industry requesting that a minimum number of versions be drafted to allow entities to have a complete set of revised requirements as soon as possible to reduce impact. Meeting both objectives has led to overlap in the posting schedule.	
Wendy Center - U.S. Bureau of Reclamation - 1,5 - WECC	
Answer	
Document Name	
Comment	
Due to the existing order to enforce CIP-003-6 with the LERC and LEAP definitions, Reclamation recommends to skip the CIP-003-6 enforcement and combine the changes to CIP-003-7 and CIP-003-TCA into CIP-003-7.	
Likes 0	

Dislikes 0	
Response	
Although the SDT acknowledges the concern, it is outside of the scope of work of the SDT.	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	

End of Report

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.

Description of Current Draft

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, Revised Critical Infrastructure Protection Reliability Standards, approving seven CIP Reliability Standards and new or modified definitions. In Order No. 822, the Commission also directed NERC to make certain modifications to those standards and definitions. On March 9, 2016, the NERC Standards Committee authorized the Standards Authorization Request (SAR) to be posted for a 30-day informal comment period from March 23 – April 21, 2016. Based on the comments received, the 2016-02 Modifications to CIP Standards Drafting Team (SDT) made minor revisions to the SAR which was posted for an additional 30-day informal comment period June 1-30, 2016.

In Order 822, the Commission stated:

> "32. After consideration of the comments received on this issue, we conclude that the adoption of controls for transient devices used at Low Impact BES Cyber Systems, including Low Impact Control Centers, will provide an important enhancement to the security posture of the bulk electric system by reinforcing the defense-in-depth nature of the CIP Reliability Standards at all impact levels. Accordingly, we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards."

The Standard Drafting Team (SDT) revised the Attachment 1 of CIP-003-TCA to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems. Attachment 1 contains and outlines the required sections of a Responsible Entity's cyber security plan(s) for its low impact BES Cyber Systems per Requirement R2. Previously, cyber security plan(s) were required to address four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. In keeping with the stakeholder approved approach to incorporate into one standard all the requirements applicable to assets containing low impact BES Cyber Systems, the SDT expanded CIP-003-TCA Attachment 1 to include a fifth area: "Transient Cyber Asset and Removable Media Malicious Code Mitigation Plan(s)". Requiring the Responsible Entity to develop and implement these plans will provide higher assurance against the propagation of malware from transient devices.

In addition, the SDT determined it necessary to revise the definition of a Transient Cyber Asset (TCA) in order to ensure applicability of security controls and provide additional clarity. As well, the revised definition accommodates use of the term for all impact levels: high, medium and low. This is important for those entities that may opt to deploy one program to manage TCAs across multiple impact level assets.

The proposed definition of a Transient Cyber Asset (TCA) is:

A Cyber Asset that is:

1. capable of transmitting or transferring executable code;
2. not included in a BES Cyber System;
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems; and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or
   - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

As proposed, Section 5 of Attachment 1 of CIP-003-TCA mandates that entities have malware protection on Transient Cyber Assets (both entity and vendor-managed) and for Removable Media. The SDT proposes that it is necessary to distinguish between the specific protections for: (i) Transient Cyber Assets managed by the Responsible Entity, (ii) Transient Cyber Assets managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media.

For Transient Cyber Assets managed by the Responsible Entity, Section 5 requires Responsible entities to use one or a combination of the following methods to mitigate the introduction of malicious code: antivirus software, application whitelisting, or some other method. The SDT recognized that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices (i.e., manage in an ongoing manner) while others have a checklist for transient devices prior to connecting them to a BES Cyber System (i.e., manage in an on-demand manner). The drafting team acknowledges both methods are effective and Section 5 permits either form of management. Because of the higher frequency in which these entity-managed devices are used, the controls required for these devices are more specific.

For Transient Cyber Assets managed by a party other than the Responsible Entity, Section 5 requires the Responsible Entity to review and verify the malware mitigation mechanism(s) used by the third party prior to connecting the Transient Cyber Asset (per Transient Cyber Asset capability).

For Removable Media, Section 5 requires entities to use methods to detect malicious code and mitigate the threat of detected malicious code prior to connecting to a low impact BES Cyber System.

In summary, the SDT made the following changes to address the directive:

1. Revised the definition of Transient Cyber Assets.
2. Revised Requirement R1, by adding Part 1.2.5 to include the complementary policy for the Transient Cyber Assets and Removable Media Malicious Code Mitigation Plan(s) in Requirement R2 (Attachment 1 of CIP-003-TCA).
3. Revised the requirement language (Requirement R2) in Attachment 1 of CIP-003-TCA by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Mitigation Plan(s).
4. Revised the associated VSLs for Requirement R2 of CIP-003-TCA.
5. Revised the evidential language of Attachment 2 of CIP-003-TCA by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Mitigation Plan(s) to complement the revised requirement language.

Completed Actions	Date
Standard Authorization Request (SAR) approved	July 20, 2016
Draft 1 of CIP-003-TCA posted for informal comment	November 1 – 18, 2016

Anticipated Actions	Date
Draft 1 of CIP-003-TCA posted for formal comment and ballot	

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-TCA

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 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 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 SPS or RAS where the SPS or 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-TCA:

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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3 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.

4.2.3.4 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-TCA.

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single

cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity;

1.2.4. Cyber Security Incident response; and

1.2.5. Transient Cyber Assets and Removable Media Malicious Code Mitigation.

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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-TCA)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-TCA)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-TCA)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-TCA)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-TCA)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented one or more incident response plans	The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR The Responsible Entity documented the determination of	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-TCA)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, but failed to document one or more Cyber Security Incident response plans according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2,	within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented and implemented electronic access controls for LERC, but failed to implement a LEAP or permit inbound and outbound access according to Requirement R2, Attachment 1, Section 3. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-TCA)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to	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. OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)	The Responsible Entity documented and implemented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to document and implement authentication of all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-TCA)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R2, Attachment 1, Section 5.3. (R2)	OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation for the introduction of malicious code for Transient Cyber	Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-TCA)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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 1, Section 5.2. (R2)	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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-TCA)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	Attachment 1, Section 5.3. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-TCA)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				50 calendar days of the change. (R3)		Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-TCA)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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

Version	Date	Action	Change Tracking
			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 devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	

Attachment 1

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

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

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

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

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall:

- **3.1** For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access; and
- **3.2** Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

- **4.1** Identification, classification, and response to Cyber Security Incidents;
- **4.2** Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;
- **4.3** Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;
- **4.4** Incident handling for Cyber Security Incidents;
- **4.5** Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security

Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Rationale for Section 5 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security control objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into a facility and subsequently into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more Transient Cyber Asset and Removable Media Malicious Code Mitigation plan(s). The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

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

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

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

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, use of one or a combination of the following methods prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;

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

5.3 For Removable Media, perform each of the following:

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

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

Attachment 2

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

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

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

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

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset, if any, containing a LEAP.

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

1. Documentation showing that inbound and outbound connections for any LEAP(s) are confined to only those the Responsible Entity deems necessary (e.g., by restricting IP addresses, ports, or services); and documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);

2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Mitigation Plan(s):

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability
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 mitigate 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.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-TCA, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-TCA, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any *assets containing low impact BES Cyber Systems*, the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-TCA, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

Using the list of assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that addresses objective criteria for the protection of low impact BES Cyber Systems. The protections required by Requirement R2 reflect the level of risk that misuse or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the required protections are part of a program that covers the low impact BES Cyber Systems

collectively either at an asset or site level (assets containing low impact BES Cyber Systems), but not at an individual device or system level.

There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and Dial-up Connectivity, and (4) Cyber Security Incident response.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. Guidance for each of the four subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The Responsible Entity is not required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or “If you see something, say something” campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) low impact BES Cyber Systems at assets containing low impact BES Cyber System(s) and (2) LEAPs, if any. If the LEAP is located within the BES asset and inherits the same controls outlined in Section 2, this can be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility in the selection of the methods used to meet the objective to control physical access to the asset(s) containing low impact BES Cyber Systems, the low impact BES Cyber Systems themselves, or LEAPs, if any. The Responsible Entity may use one or a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

The objective is to control the physical access based on need as determined by the Responsible Entity. The need can be documented at the policy level for access to the site or systems, including LEAPs. The requirement does not obligate an entity to specify a need for each access or authorization of a user for access.

Monitoring as a physical security control can be used as a complement or an alternative to access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of boundary protections for *low impact BES Cyber Systems* when the low impact BES Cyber Systems have bi-directional routable protocol communication or Dial-up Connectivity to devices external to the asset containing the low impact BES Cyber Systems. The establishment of boundary protections is intended to control communication either into the asset containing low impact BES Cyber System(s) or to the low impact BES Cyber System itself to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. The term "electronic access control" is used in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing. The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or Dial-up Connectivity present. In the case where there is no external bi-directional routable protocol communication, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s).

The defined terms LERC and LEAP are used to avoid confusion with the similar terms used for high and medium impact BES Cyber Systems (e.g., External Routable Connectivity (ERC) or Electronic Access Point (EAP)). To future-proof the standards, and in order to avoid future technology issues, the definitions specifically exclude "point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems," such as IEC 61850 messaging. This does not exclude Control Center communication but rather excludes the communication between the intelligent electronic devices themselves. A Responsible Entity using this technology is not expected to implement a LEAP. This exception was included so as not to inhibit the functionality of the time-sensitive requirements related to this technology nor to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

When determining whether there is LERC to the low impact BES Cyber System, the definition uses the phrases "direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection." The intent of "direct" in the definition is to indicate LERC exists if a person is sitting at another device outside

of the asset containing the low impact BES Cyber System, and the person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session even if there is a serial-to-routable protocol conversion. The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for "device-to-device connection," LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication to or from the low impact BES Cyber System.

When identifying a LEAP, Responsible Entities are provided flexibility in the selection of the interface on a Cyber Asset that controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, the internal interface on a router that has implemented an access control list (ACL), or other security device. The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required to reside at the asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP per asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber Systems. Locating the Cyber Asset with multiple LEAPs at an external location with multiple assets containing low impact BES Cyber Systems "behind" it, however, should not allow uncontrolled access to assets containing low impact BES Cyber Systems sharing a Cyber Asset containing the LEAP(s).

In Reference Model 4, the communication flows through an IP/Serial converter. LERC is correctly identified in this Reference Model because the IP/Serial converter in this instance is doing nothing more than extending the communication between the low impact BES Cyber System and the Cyber Asset outside the asset containing the low impact BES Cyber System. In contrast, Reference Model 6 has placed a Cyber Asset that performs a complete break or interruption that does not allow the user or device data flow to directly communicate with the low impact BES Cyber System. The Cyber Asset in Reference Model 6 is preventing extending access to the low impact BES Cyber System from the Cyber Asset outside the asset containing the low impact BES Cyber System. The intent is that if the IP/Serial converter that is deployed only does a "pass-through" of the data flow communication, then that "pass-through" data flow communication is LERC and a LEAP is required. However, if that IP/Serial converter performs some type of authentication in the data flow at the asset containing the low impact BES Cyber System before the communication can be sent to the low impact BES Cyber System, then that type of IP/Serial converter implementation is not LERC.

A Cyber Asset that contains interface(s) that only perform the function of a LEAP does not meet the definition of Electronic Access Control or Monitoring System (EACMS) associated with medium or high impact BES Cyber Systems and is not subject to the requirements applicable to an EACMS. However, a Cyber Asset may contain some interfaces that function as a LEAP and other interfaces that function as an EAP for high or medium impact BES Cyber Systems. In this case, the Cyber Asset would also be subject to the requirements applicable to the EACMS associated with the medium or high impact BES Cyber Systems.

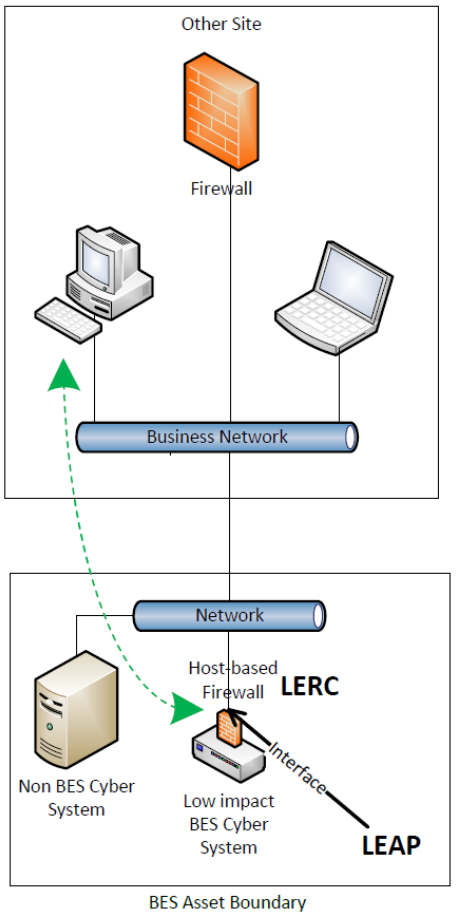
Examples of sufficient access controls may include:

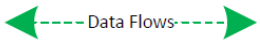
- Any LERC for the asset passes through a LEAP with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g., IP addresses, ports, or services).
- As shown in Reference Model 1 below, the low impact BES Cyber System has a host-based firewall that is controlling the inbound and outbound access. In this model, it is also possible that the host-based firewall could be on a non-BES Cyber Asset. The intent is that the host-based firewall controls the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in the business network.
- As shown in Reference Model 5 below, a non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that the non-BES Cyber Asset has provided a "protocol break" so that access to the low impact BES Cyber System is only from the non-BES Cyber Asset that is located within the asset containing the low impact BES Cyber System.
- Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- An asset has LERC due to a BES Cyber System within it having a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- In Reference Model 5, using just dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System and the business network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security device on that non-BES Cyber Asset.

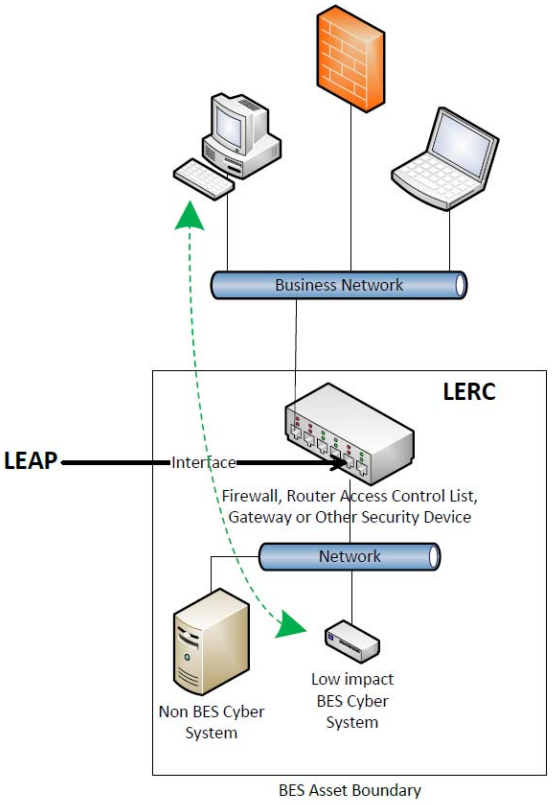
The following diagrams provide reference examples intended to illustrate how to determine whether there is LERC and for implementing a LEAP. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.





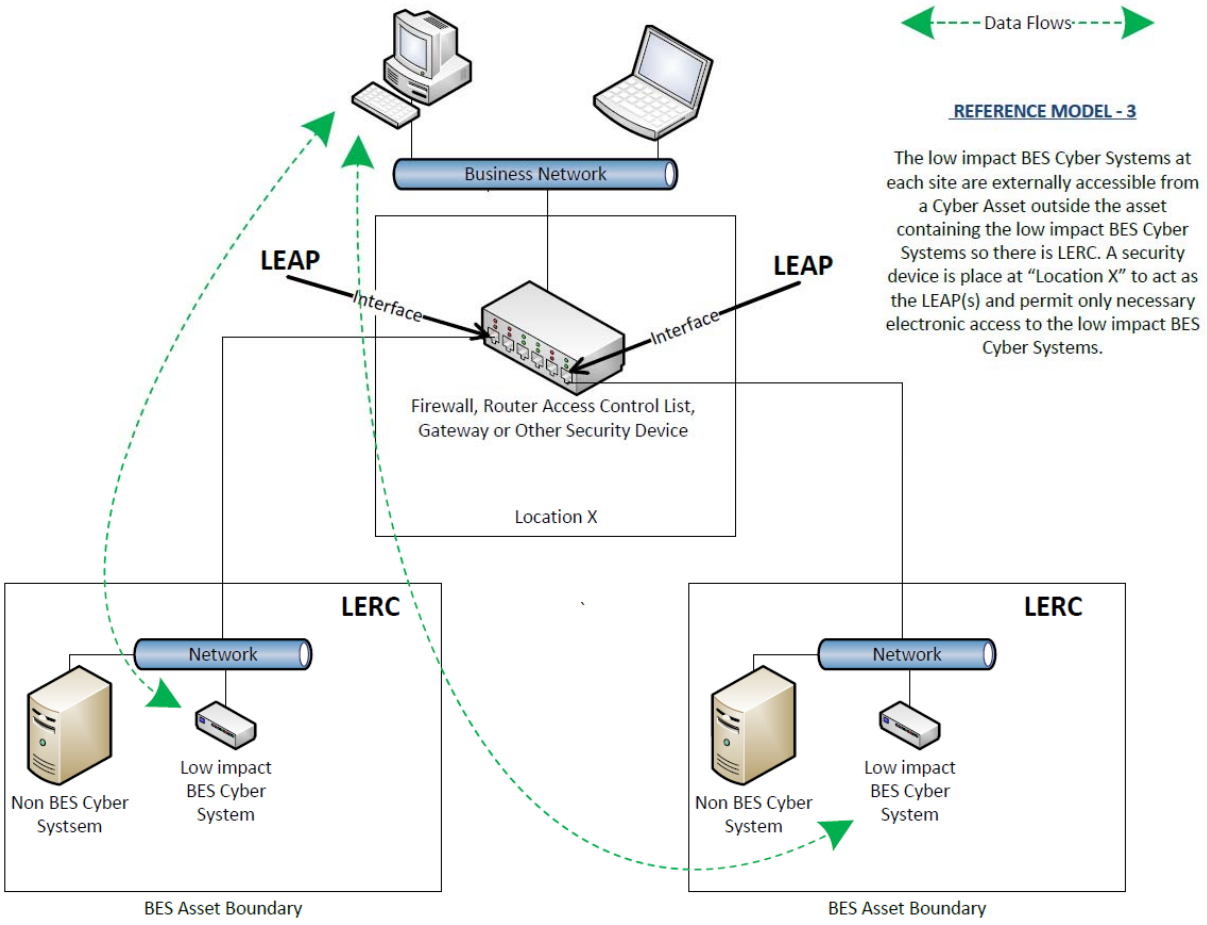
REFERENCE MODEL - 1

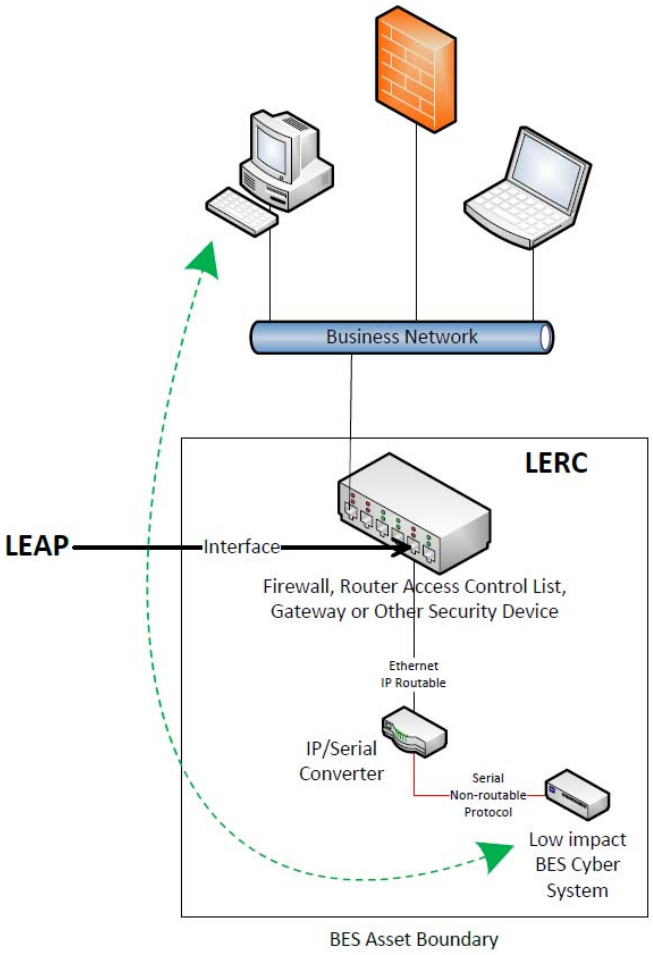
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A host-based firewall is configured on the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.



REFERENCE MODEL - 2

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.

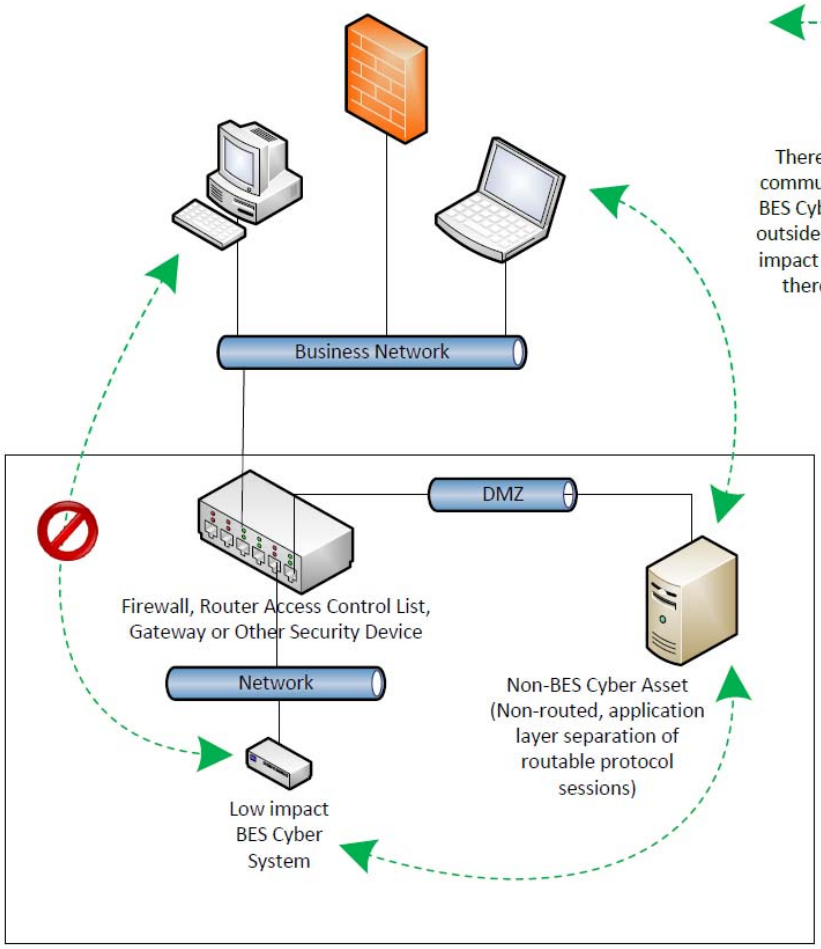

Data Flows
REFERENCE MODEL - 3
The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is place at "Location X" to act as the LEAP(s) and permit only necessary electronic access to the low impact BES Cyber Systems.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Location X
LERC
Network
Non BES Cyber Systsem
Low impact BES Cyber System
BES Asset Boundary
LERC
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

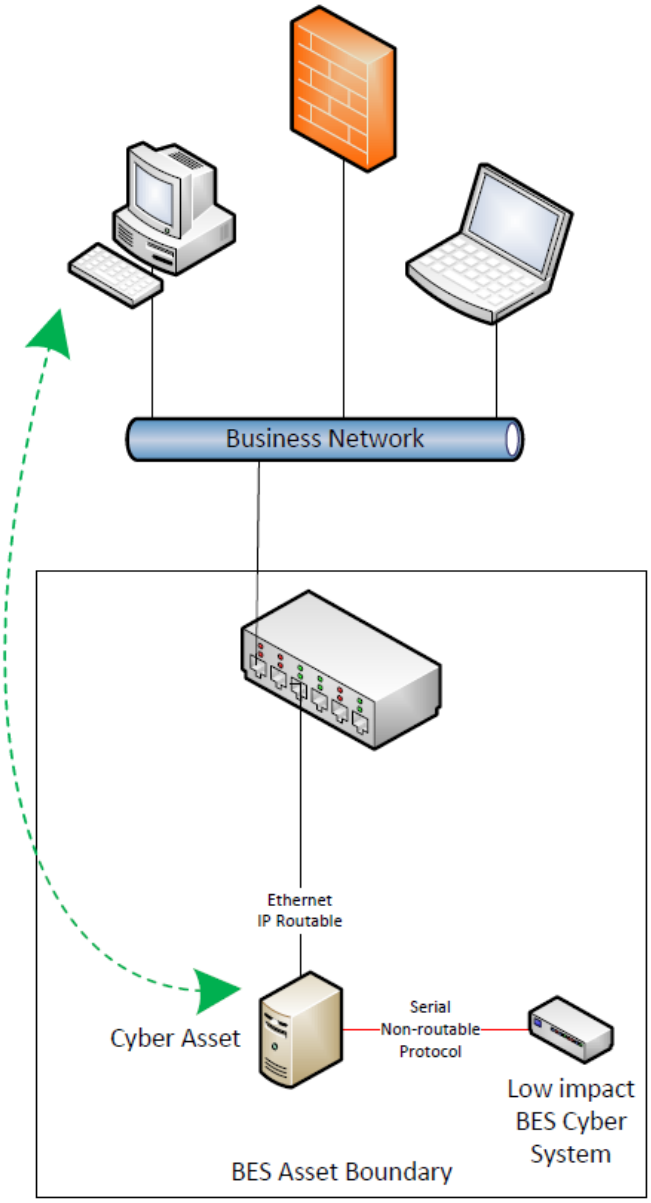


Data Flows

REFERENCE MODEL - 4

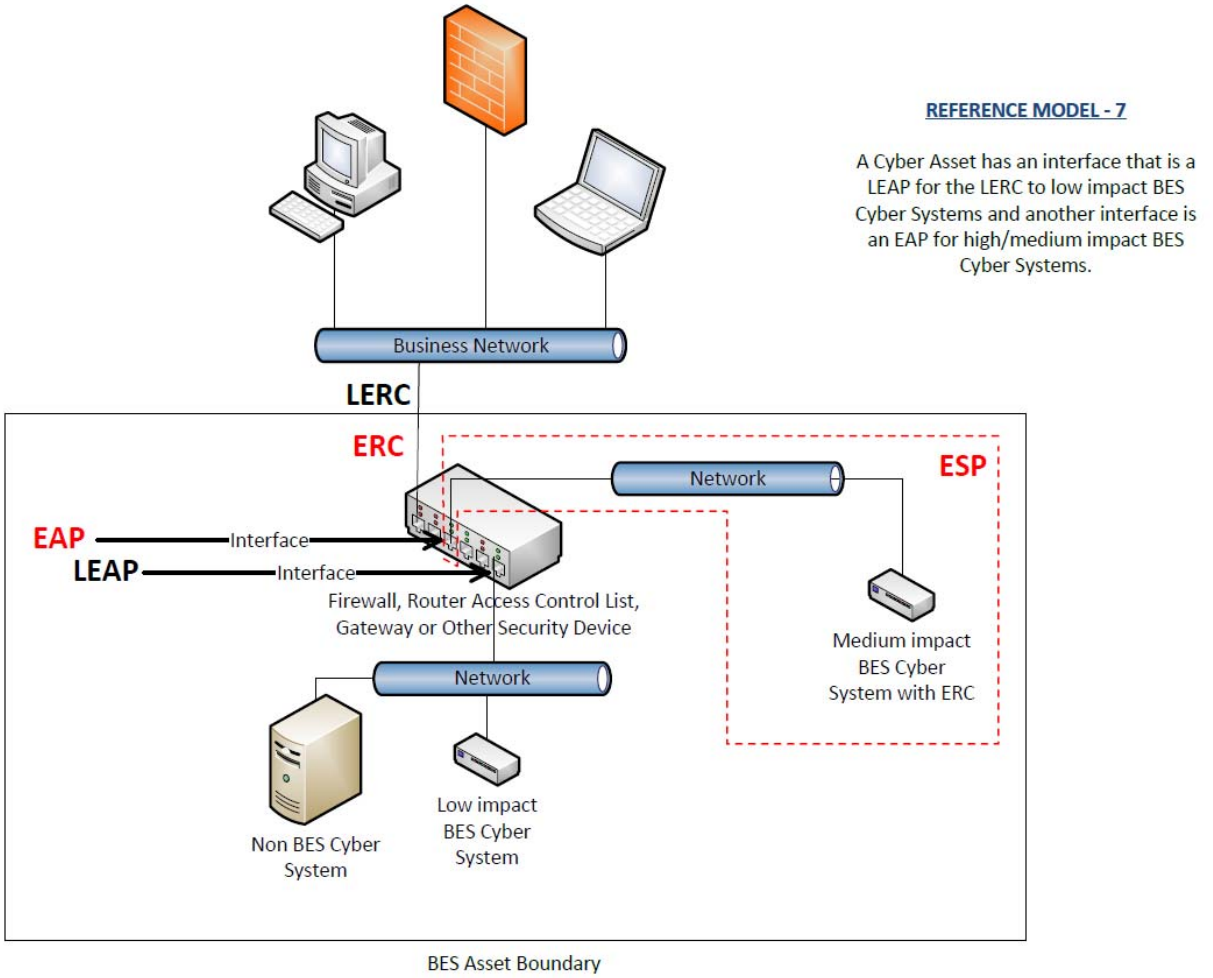
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.


Data Flows
REFERENCE MODEL - 5
There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.
Business Network
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset (Non-routed, application layer separation of routable protocol sessions)
Low impact BES Cyber System
BES Asset Boundary



REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.



Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident

response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, “A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.” The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Mitigation Plan(s)

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore require Transient Cyber Assets and Removable Media to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003, R2 Attachment 1, Section 5 requires entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation in this context does not require that each vulnerability be individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and should consider managing these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the Transient Cyber Asset. When addressing malicious code protection, the Responsible Entity should address methods deployed to mitigate the introduction of malicious code. The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of a managed device in an on-going manner is one that has an antivirus solution that is managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. An example of managing a device in an on-demand manner may be for devices that are used infrequently whereas the signatures or patterns are not kept current which requires an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code. Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to ensure that the Transient Cyber Asset is meeting the objective to mitigate the introduction of malicious code. It is not intended that a Responsible Entity conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-TCA, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-TCA, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System. The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System. However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has “the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

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.

Description of Current Draft

This draft of CIP-003-7 is addressing the directive issued by the Federal Energy Regulatory Commission (Commission) in paragraph 73 of Order No. 822 which reads:

> [T]he Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule approving revisions to the cybersecurity Critical Infrastructure Protection (CIP) standards.

In this revision, the SDT revised Sections 2 and 3 of Attachments 1 and 2 ~~in~~to CIP-003-7 and removed the terms Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP). The modifications incorporate concepts and select language from the LERC definition into Attachment 1, Section 3 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). The SDT simplified Section 3 of Attachment 1 to require the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii) which reads: "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The defined term LEAP is no longer necessary because the SDT changed the requirement from requiring a LEAP to requiring electronic access controls. Additionally, since the SDT is removing the term LERC, the exclusion language that was previously in the definition of LERC was integrated into the Attachment 1, Section 3.1 requirement.

Because the proposed modifications ~~to~~in Reliability Standard CIP-003-7 eliminate the need for the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP), NERC is requesting these terms be retired in the associated Implementation Plan.

~~Additionally, the SDT:~~

- ~~revised the associated Lower, Moderate, and High VSLs for Requirement R2 to complement the requirement revisions;~~
- ~~corrected a mistake in the Severe VSL for Requirement R2;~~
- ~~made non-substantive changes to the Moderate and High VSLs for Requirement R2 to align with the order of the requirement;~~
- ~~removed repetitive text from Requirement R1, Part 1.2.3 to make it consistent with Parts 1.2.1 and 1.2.2;~~

~~updated the Guidelines and Technical Basis section of the standard to reflect the revisions made to the Attachments; and~~

- ~~made non-substantive errata changes throughout the standard such as replacing "ES-ISAC" with "E-ISAC".~~

Completed Actions	Date
Standard Authorization Request (SAR) approved	July 20, 2016
Draft 1 of CIP-003-7 posted for formal comment and initial ballot	July 21 – September 6, 2016
Draft 2 of CIP-003-7 posted for formal comment and additional ballot	October 21 – December 5, 2016
10-day final ballot	December 9-19, 2017

Anticipated Actions	Date
~~10-day final ballot~~	~~January, 2017~~
NERC Board of Trustees (BOT) adoption	February, 2017
Petition filed with FERC	March, 2017

A. Introduction

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

2. **Number:** CIP-003-7

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 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 SPS or RAS where the SPS or 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-003-7:

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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3 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.

4.2.3.4 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-003-7.

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single

cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls; and

1.2.4. Cyber Security Incident response

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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate

implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans	containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented	failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2)	its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification,	The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(E-ISAC) according to Requirement R2, Attachment 1, Section 4.		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but	The Responsible Entity has used delegated authority for actions where allowed by the CIP

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specific actions delegated, but 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. (R4)	specific actions delegated, but 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. (R4)	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. (R4)	Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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.	

Version	Date	Action	Change Tracking
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 devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees.	Revised to address FERC Order 822 directive regarding definition of LERC.

Attachment 1

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

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

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

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

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security ~~control~~ objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term ~~"direct"~~'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule~~."~~."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii~~) which reads:~~): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The

focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

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

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

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

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and~~,~~

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g.~~,~~ communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Attachment 2

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

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

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

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

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

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

1. Documentation~~, such as representative diagrams or lists of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; implementing unidirectional gateways)~~ showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices~~; and~~ . Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of

implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible ~~Entity is not~~Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this ~~can~~may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a

combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The ~~requirement does~~standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). ~~The~~The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities ~~are~~ to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such

communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, ~~any~~it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), ~~does not require evaluation~~to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

~~In order for Responsible Entities to~~To determine whether electronic access controls need to be implemented, the Responsible Entity ~~needs~~has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that ~~use~~uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach ~~to making this evaluation.~~. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the

Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity ~~documents~~to document and ~~implements~~implement its chosen electronic access control(s). The control(s) ~~must~~are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. ~~The~~However the Responsible Entity ~~must be~~chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for ~~the~~ "necessary" inbound and outbound electronic access controls ~~can~~may be documented within the Responsible Entity's cyber security plan(s~~)~~), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

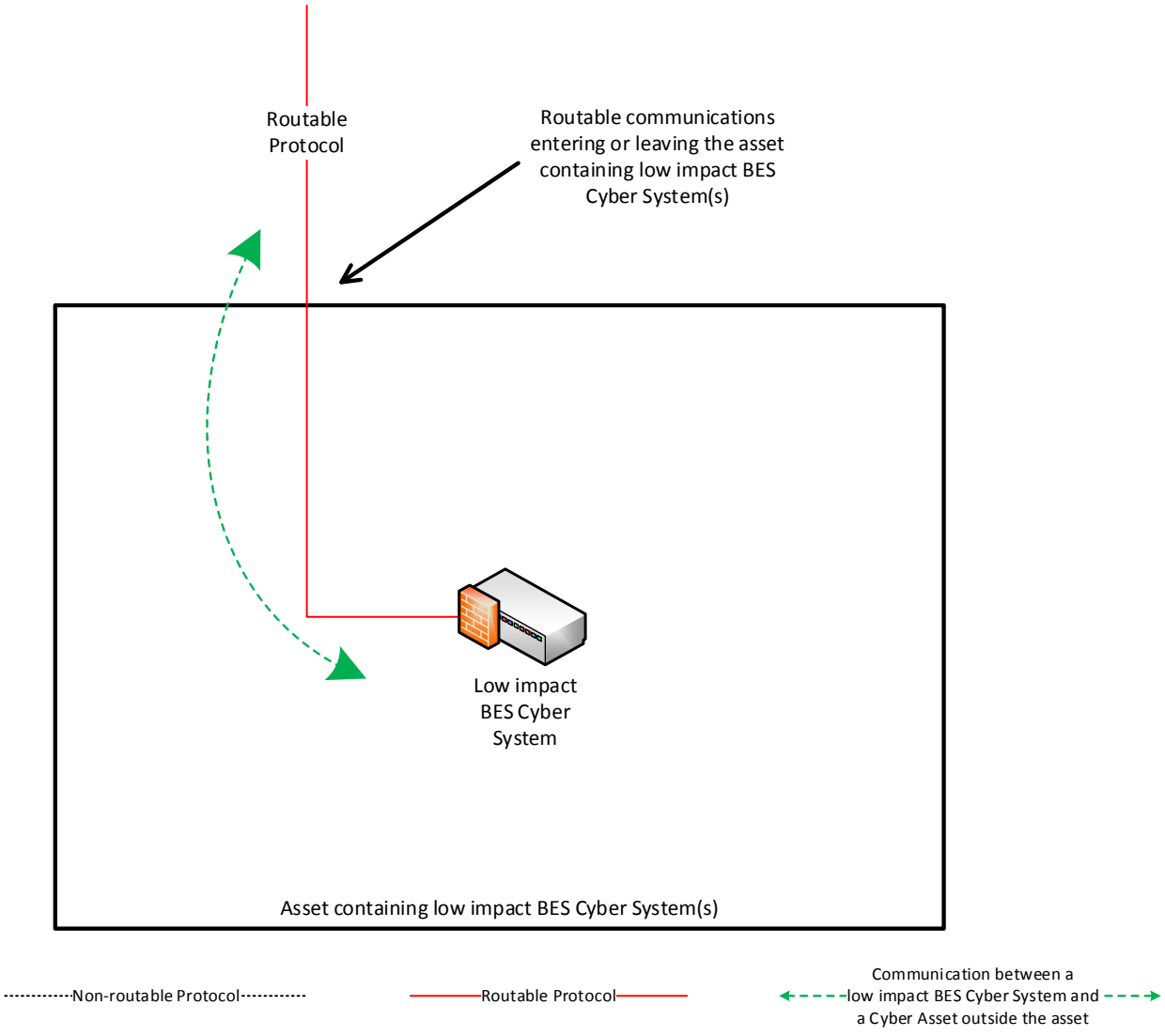
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset ~~must be met~~.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

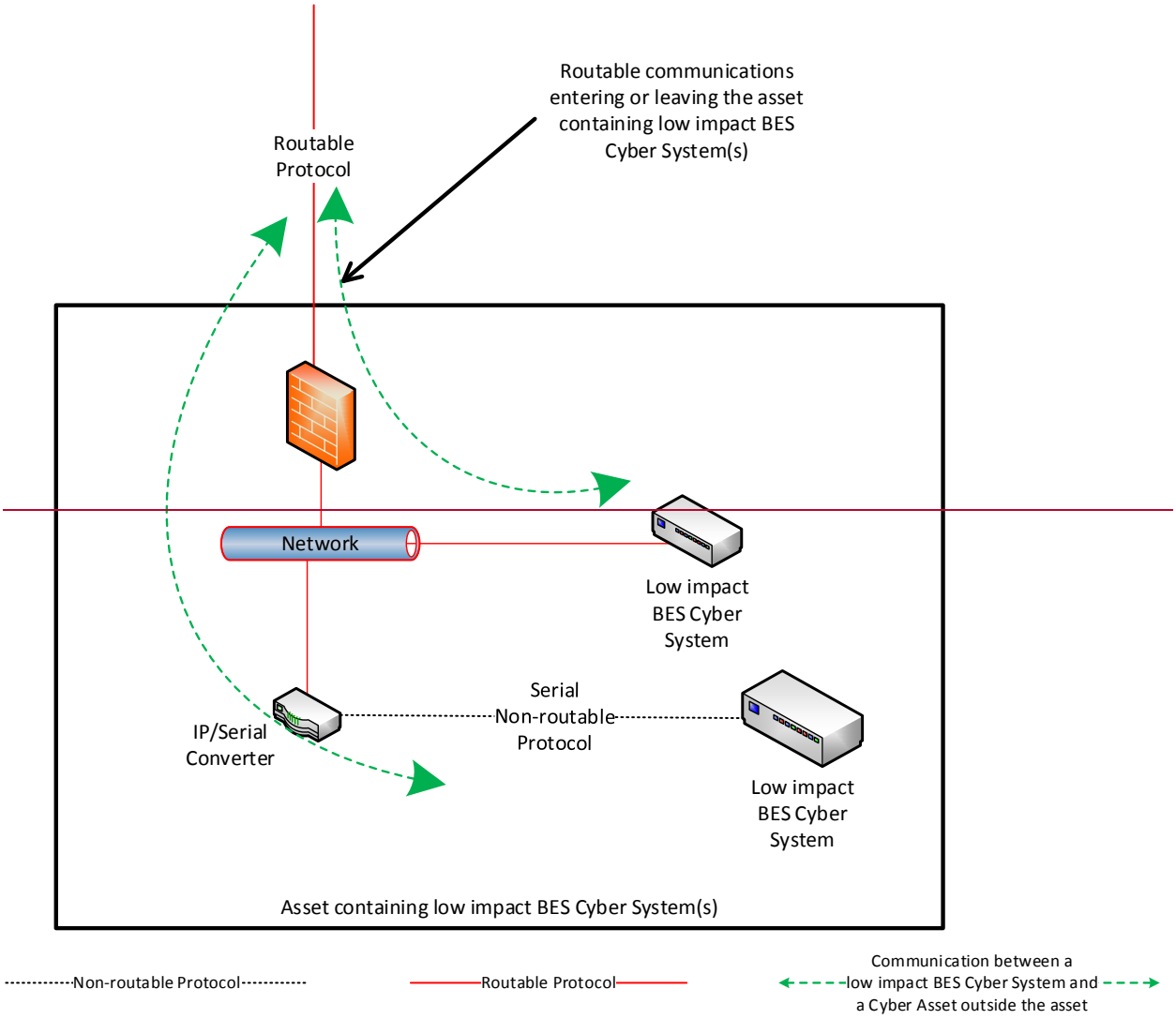
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound ~~routable protocol~~electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions~~, at a minimum~~ using access control lists, the ~~permissions need to~~Responsible Entity could restrict communication(s) using source and destination addresses~~,~~ or ~~a range~~ranges of addresses ~~when necessary.~~. Responsible Entities ~~may further~~could also restrict ~~electronic access~~communication(s) using ports ~~and~~or services based on the capability of the electronic access control, the low impact BES Cyber System~~,~~(s), or the application~~, etc.~~(s).

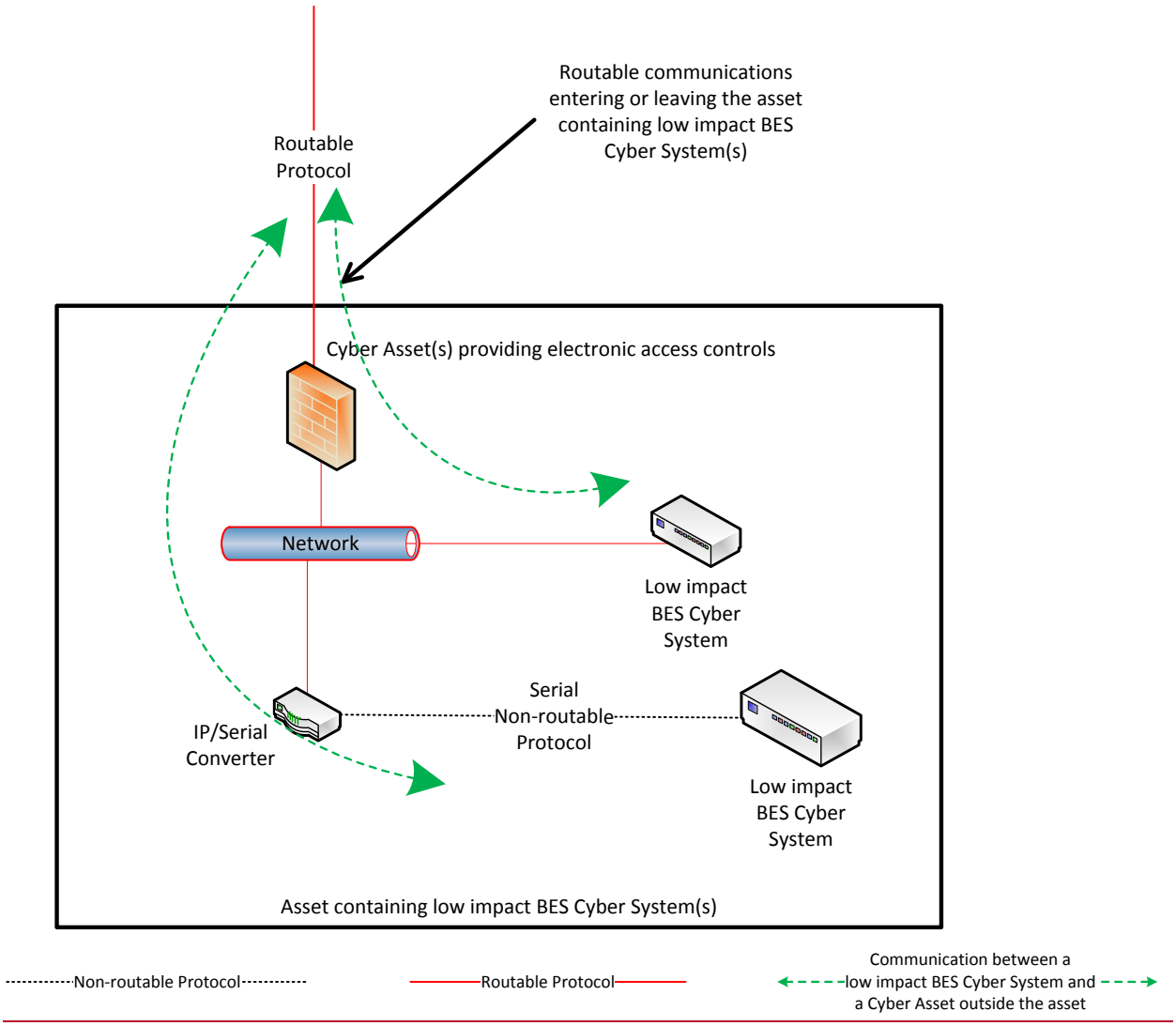


Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions~~, at a minimum~~ using access control lists, the ~~permissions need to~~Responsible Entity could restrict communication(s) using source and destination addresses~~,~~ or ~~a range~~ranges of addresses~~ when necessary.~~. Responsible Entities ~~may further~~could also restrict ~~electronic access~~communication(s) using ports ~~and~~or services based on the capability of the electronic access control, the low impact BES Cyber System~~,~~(s), or the application~~, etc.~~(s).

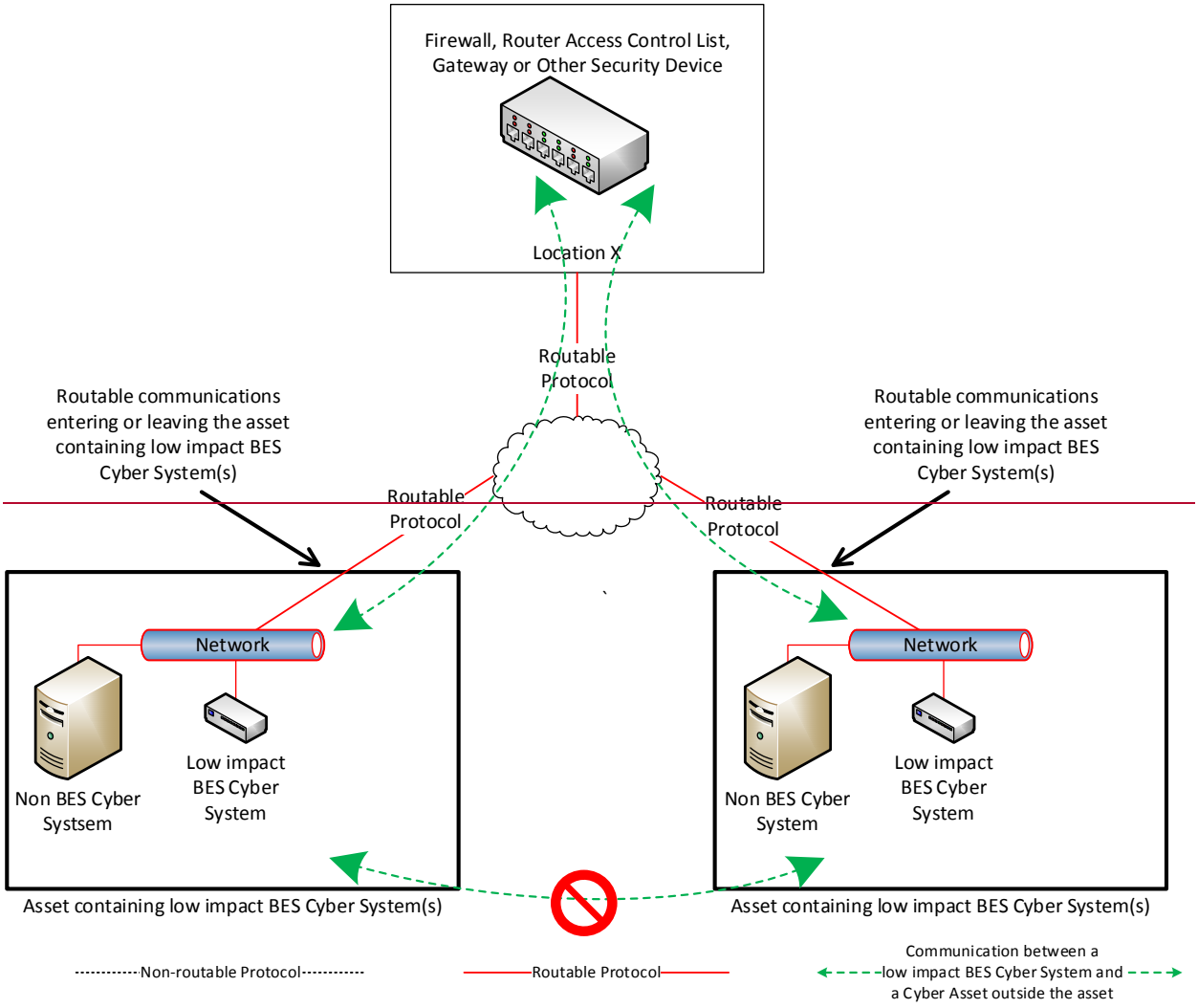


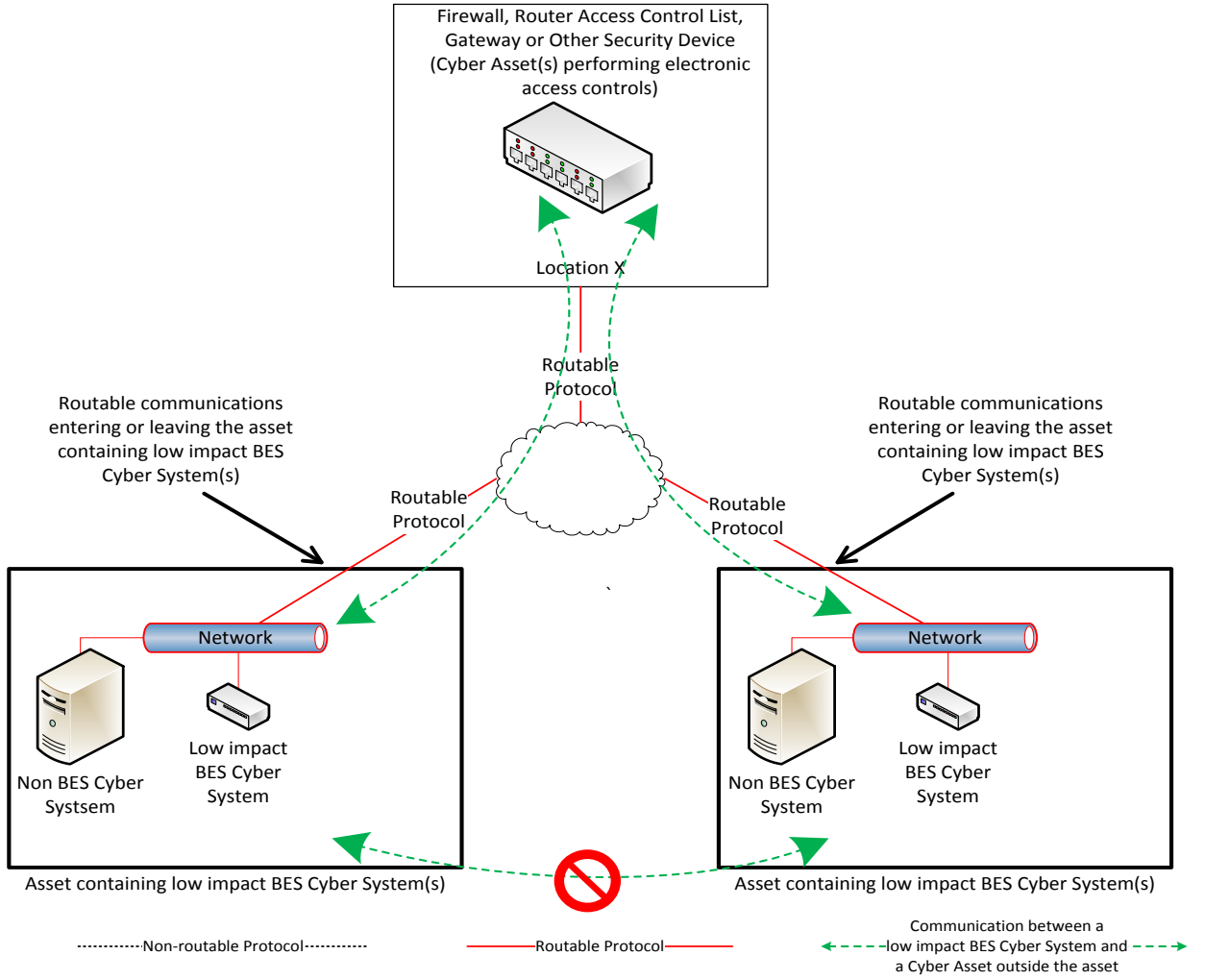


Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions~~, at a minimum~~ using access control lists, the ~~permissions need to~~Responsible Entity could restrict communication(s) using source and destination addresses~~,~~ or ~~a range~~ranges of addresses~~ when necessary.~~. Responsible Entities ~~can further~~could also restrict ~~electronic access~~communication(s) using ports ~~and~~or services based on the capability of the electronic access control, the low impact BES Cyber System~~,~~(s), or the application~~, etc.~~(s).

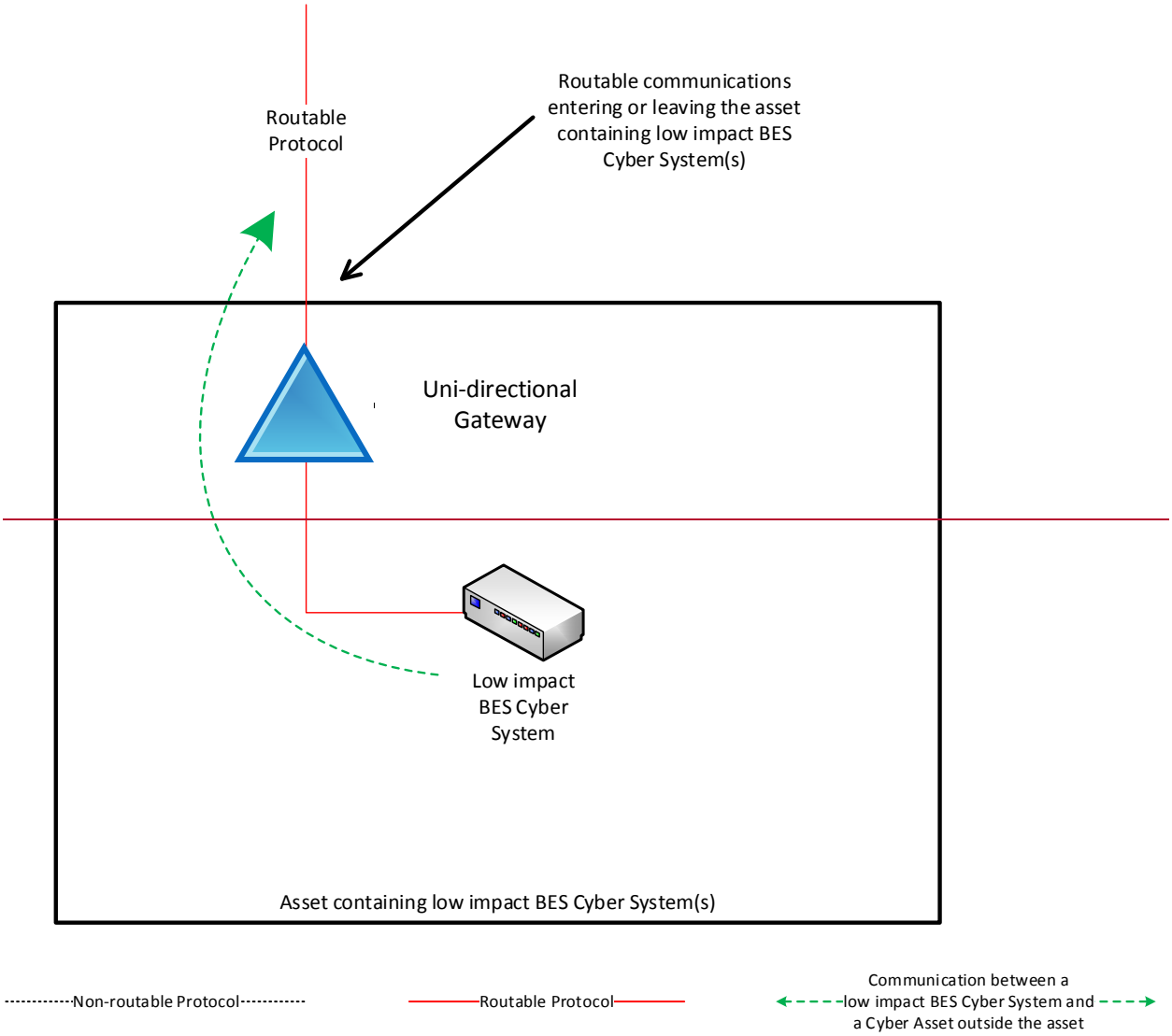

Firewall, Router Access Control List, Gateway or Other Security Device
Location X
Routable Protocol
Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
Routable Protocol
Routable Protocol
Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
Network
Non BES Cyber Systsem
Low impact BES Cyber System
Network
Non BES Cyber System
Low impact BES Cyber System
Asset containing low impact BES Cyber System(s)
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

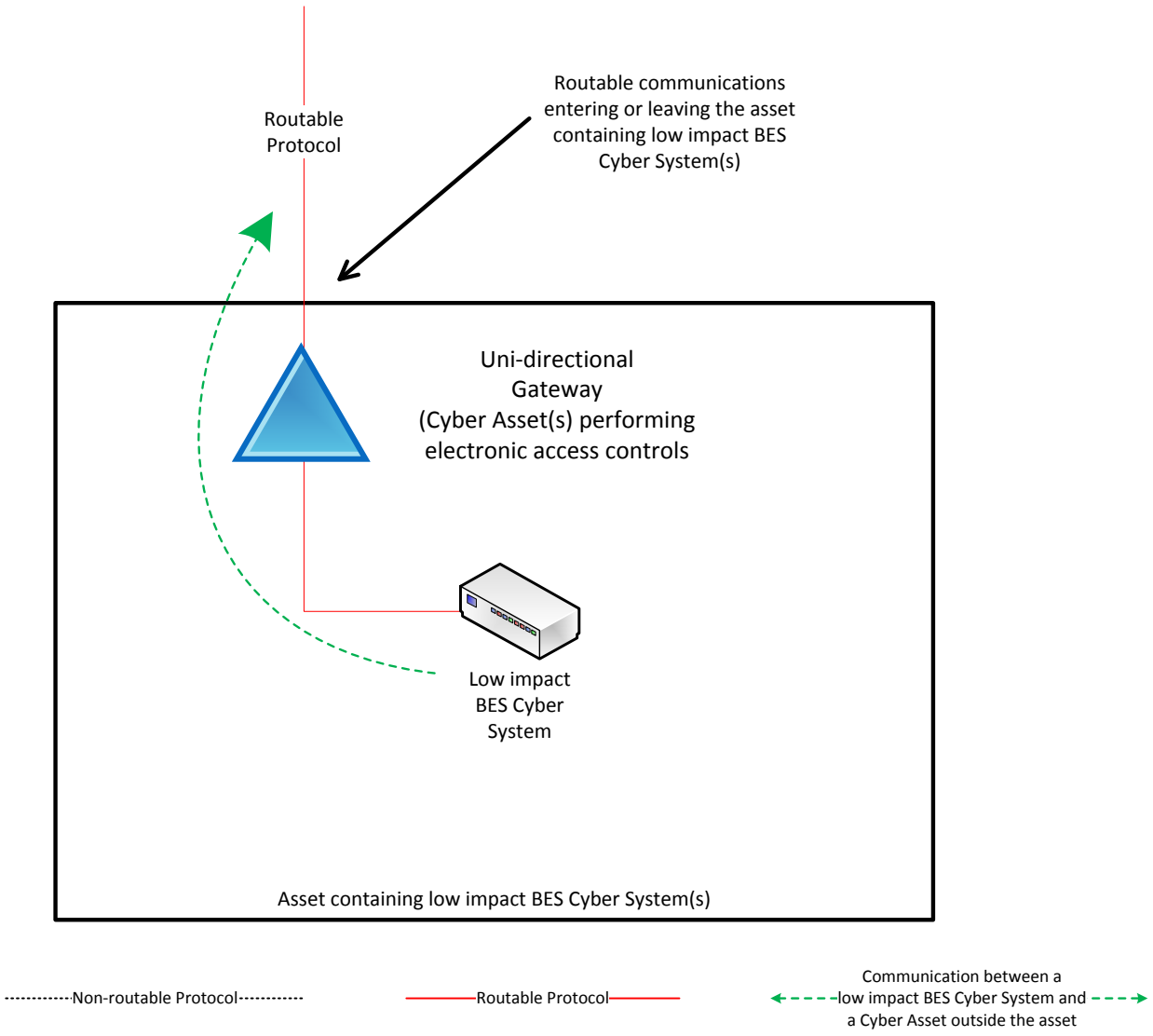


Reference Model 3

Reference Model 4 – Uni-directional Gateway

The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.

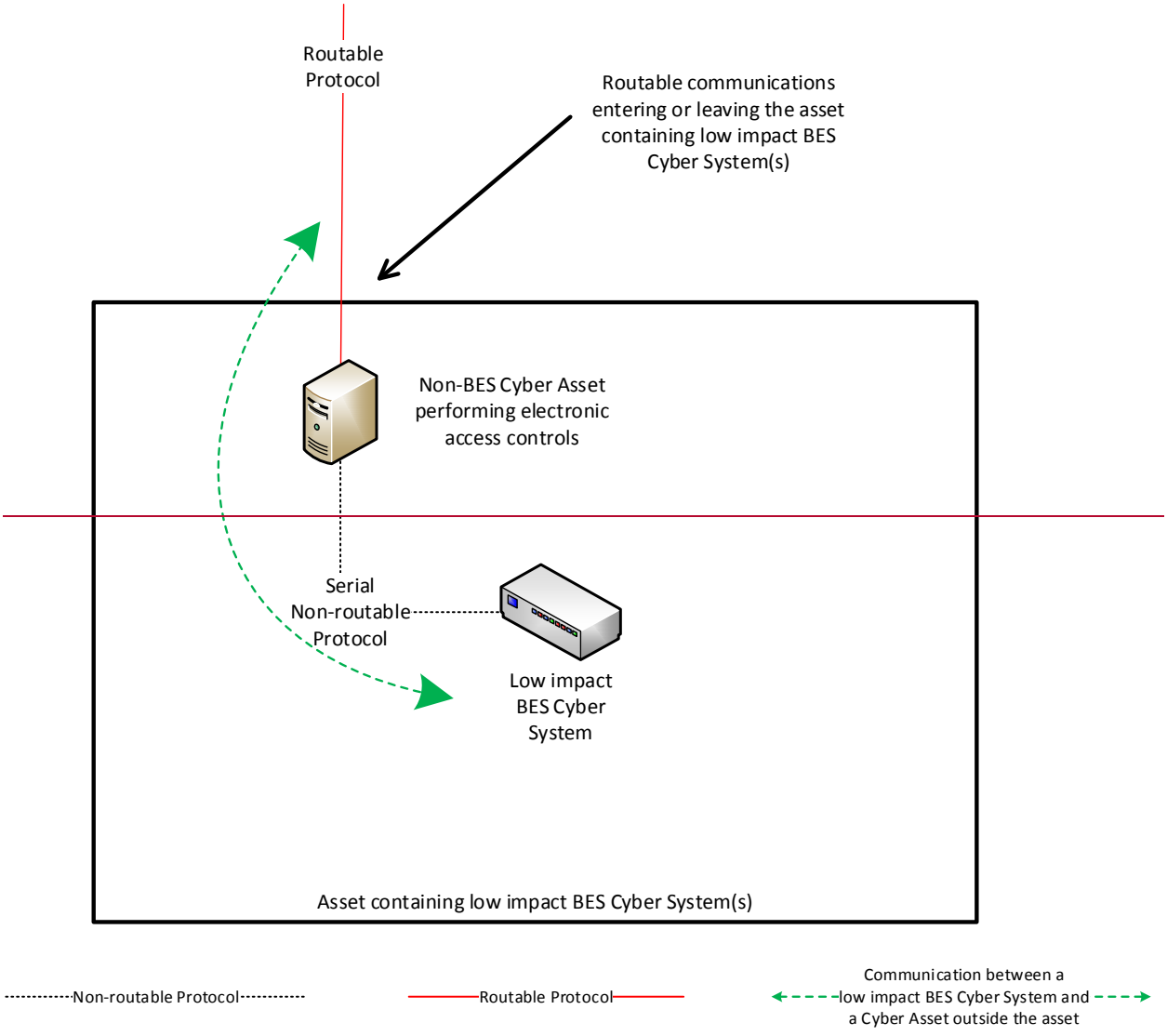


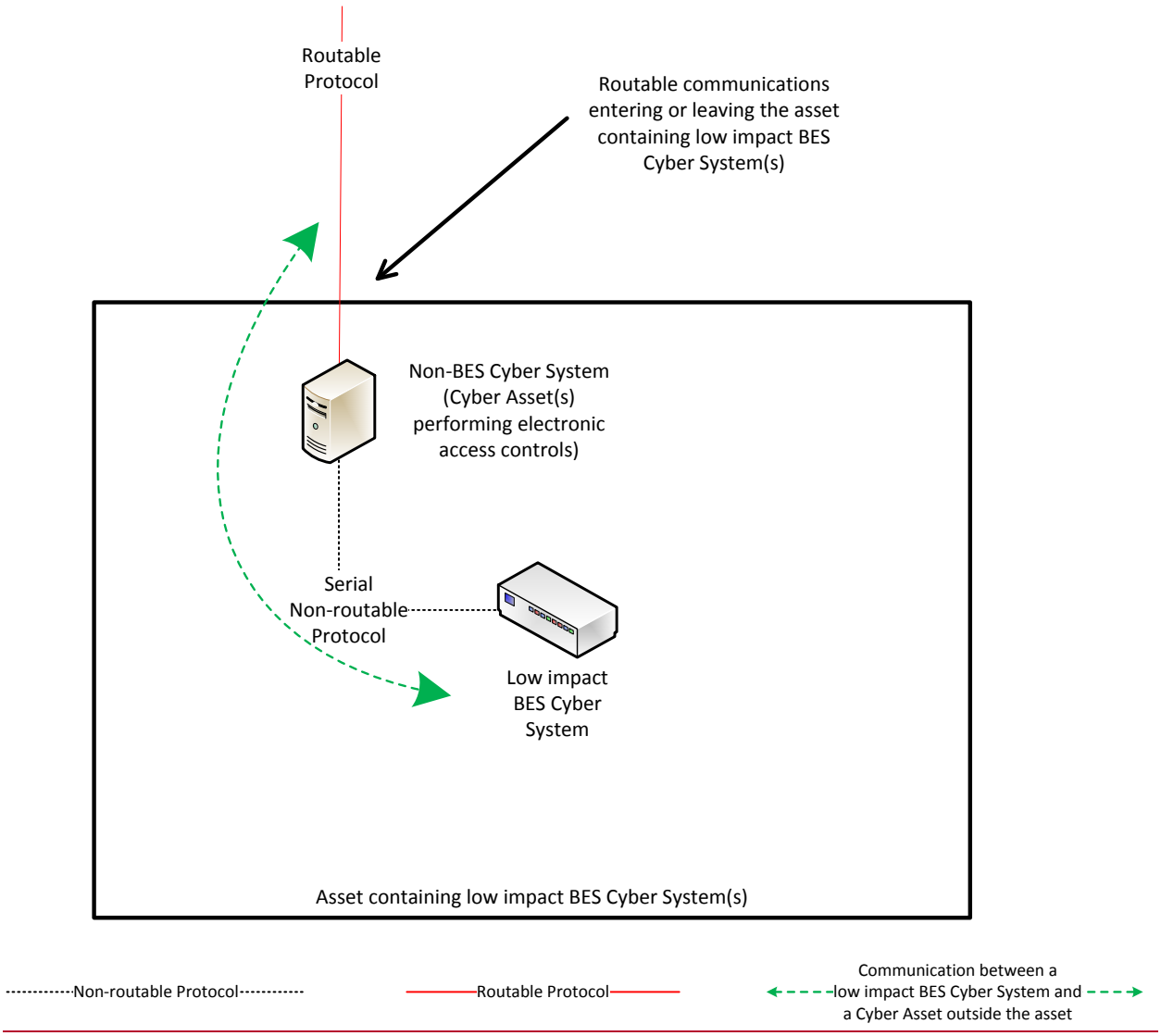


Reference Model 4

Reference Model 5 – User Authentication

This reference model demonstrates that Responsible Entities have flexibility in choosing ~~their~~ electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication ~~must be~~is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications ~~may~~would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.

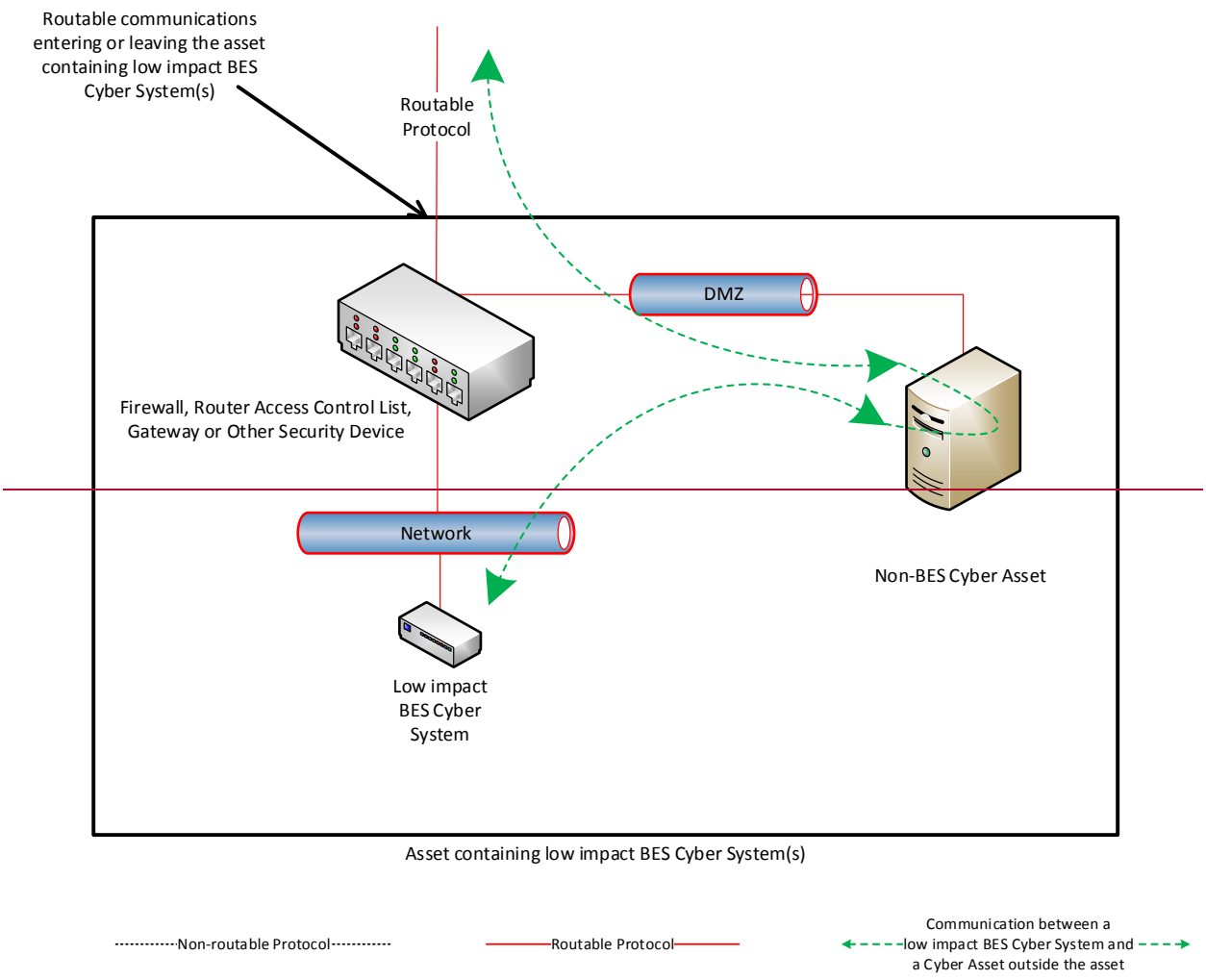


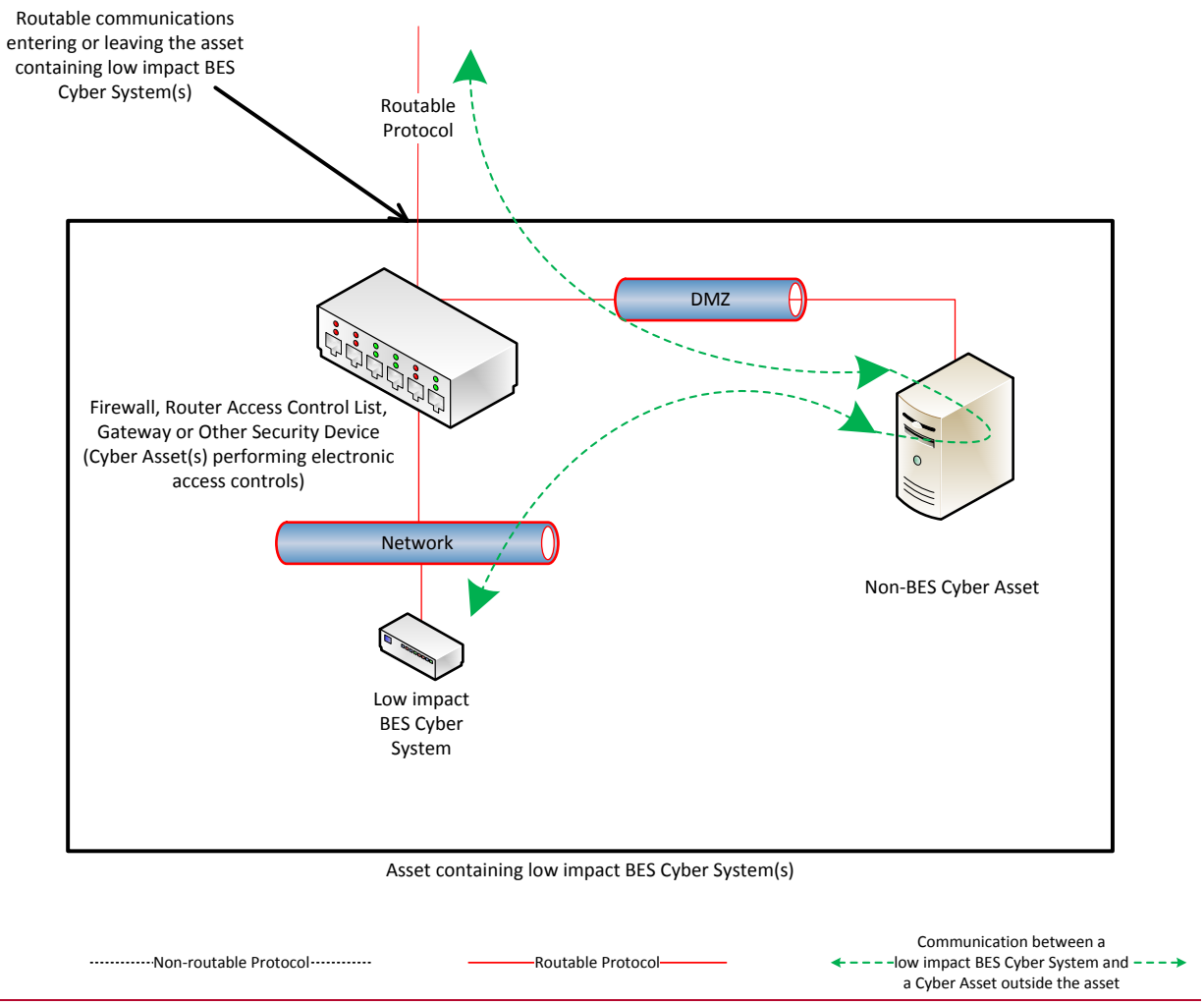


Reference Model 5

Reference Model 6 – Indirect Access

In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity ~~needs to~~ implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, ~~this~~the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.

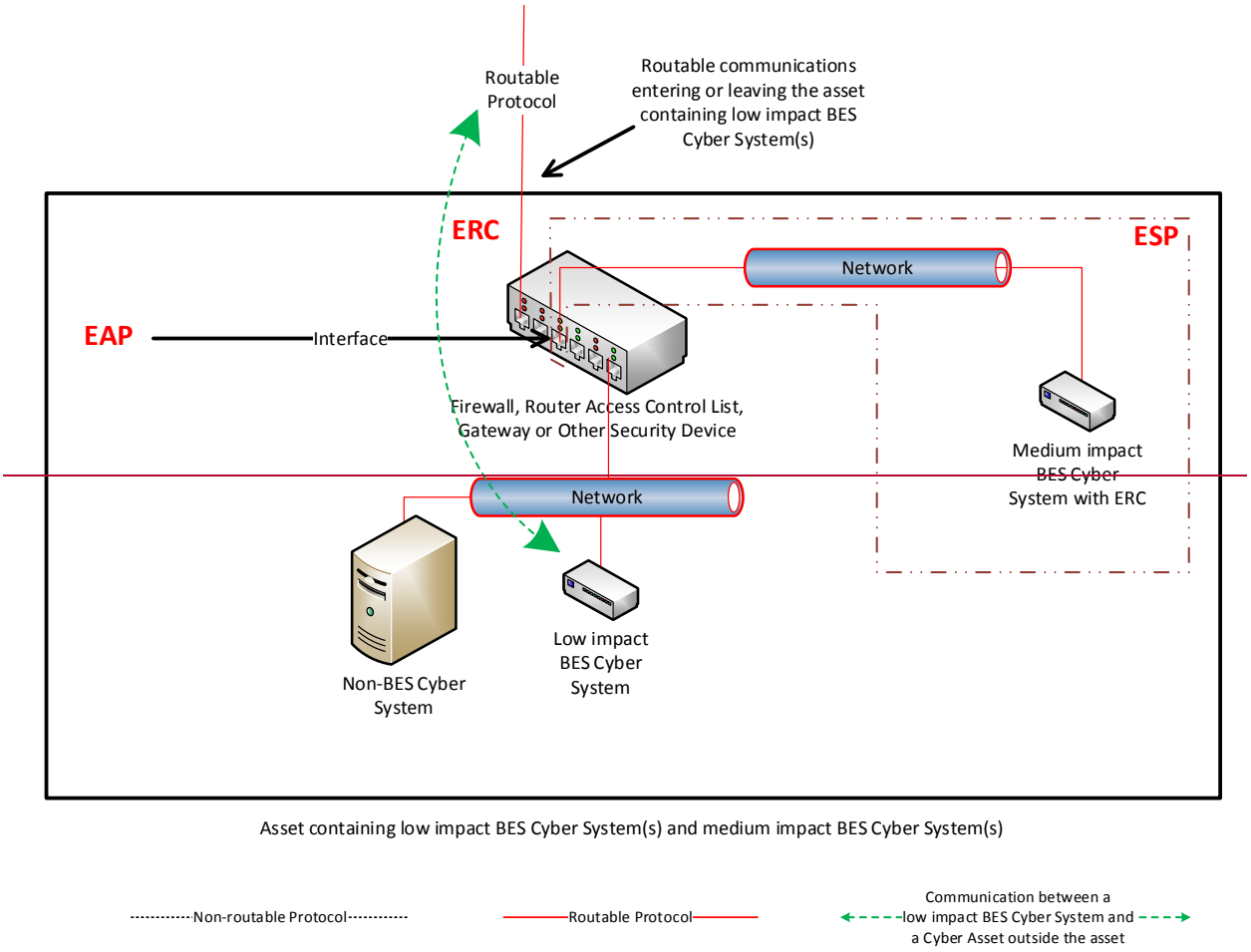

Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
Routable Protocol
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset
Low impact BES Cyber System
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

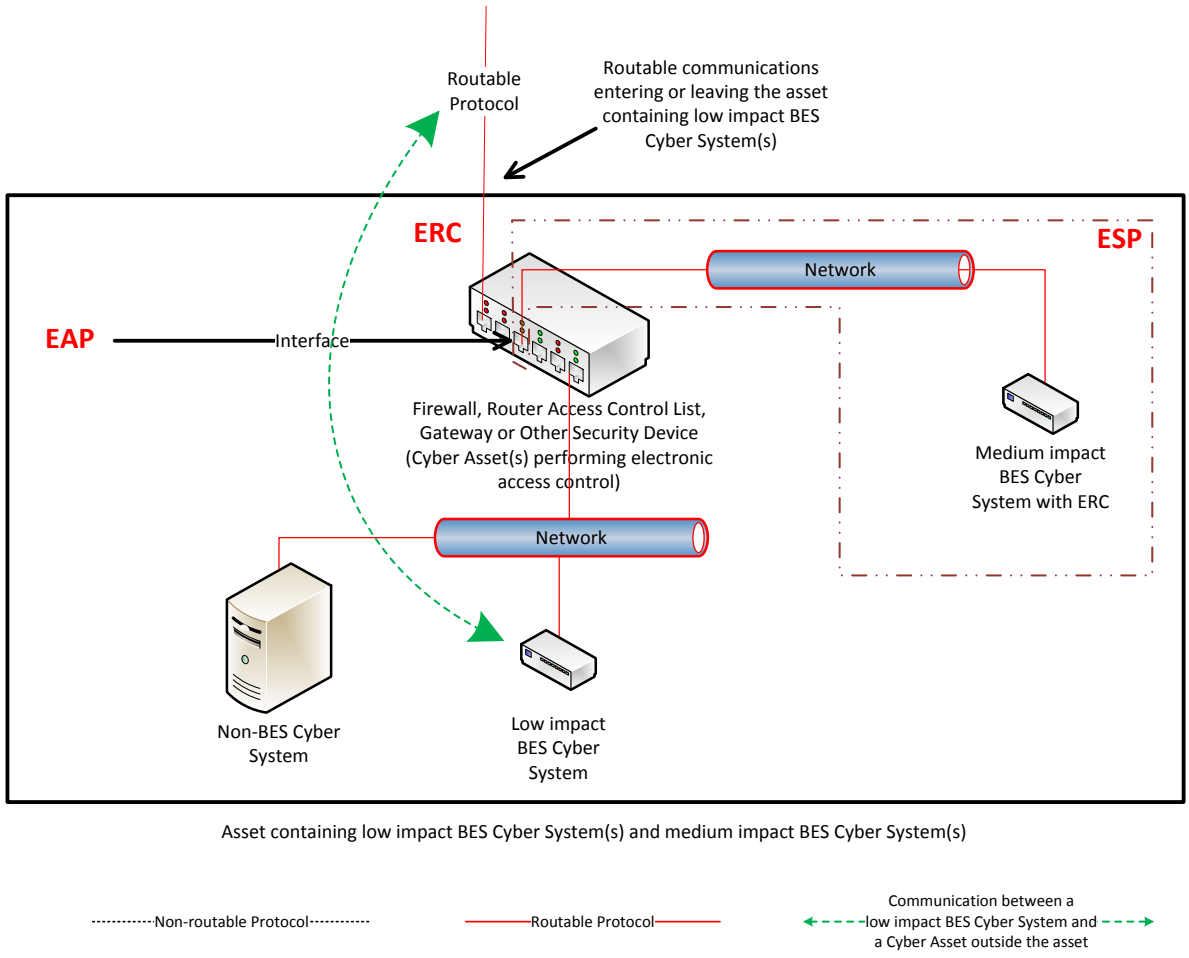


Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

~~There~~In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and ~~ERC present in this reference model~~External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls~~.~~ for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.





Reference Model 7

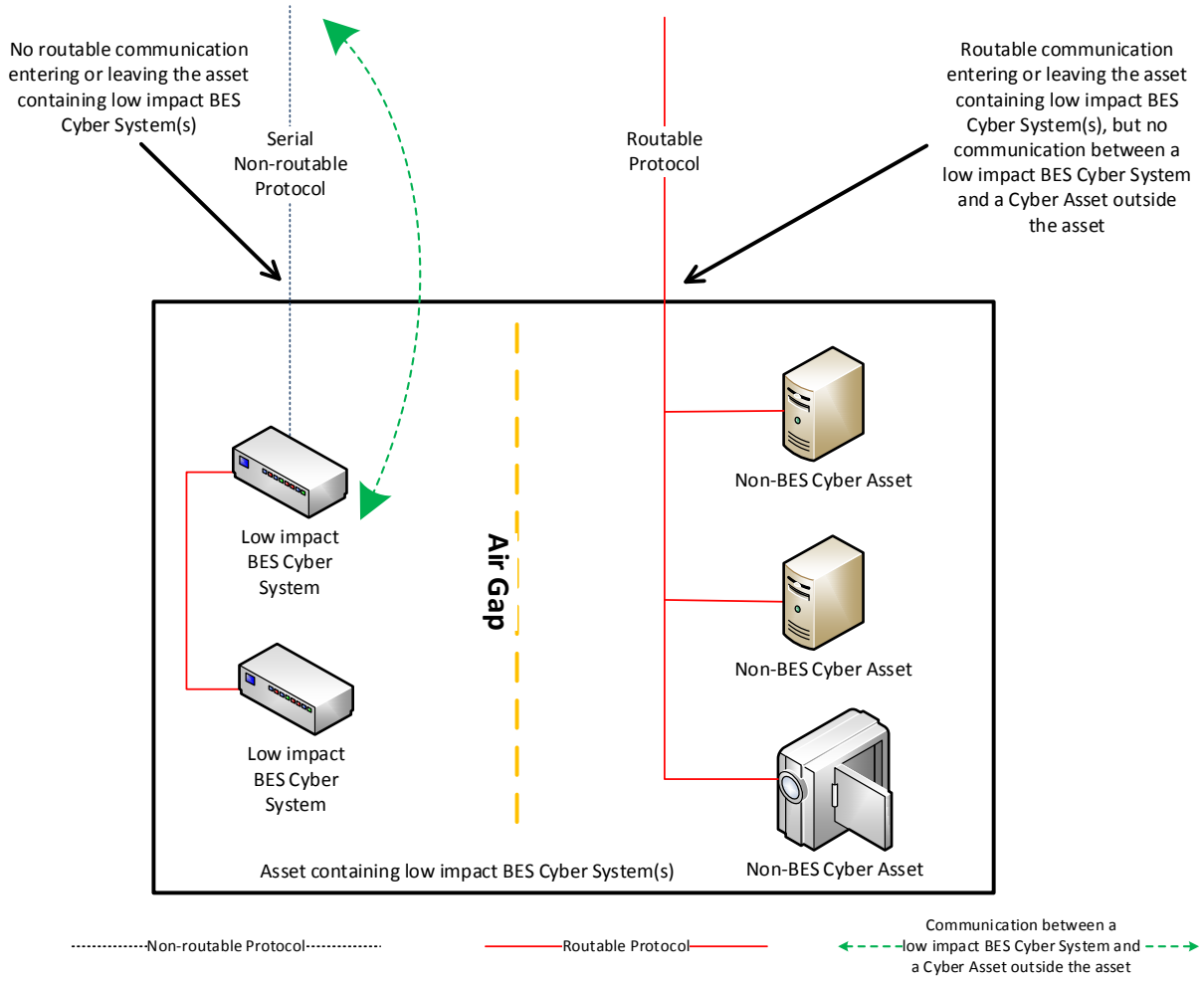
Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria ~~for~~from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;

2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls~~; and~~.

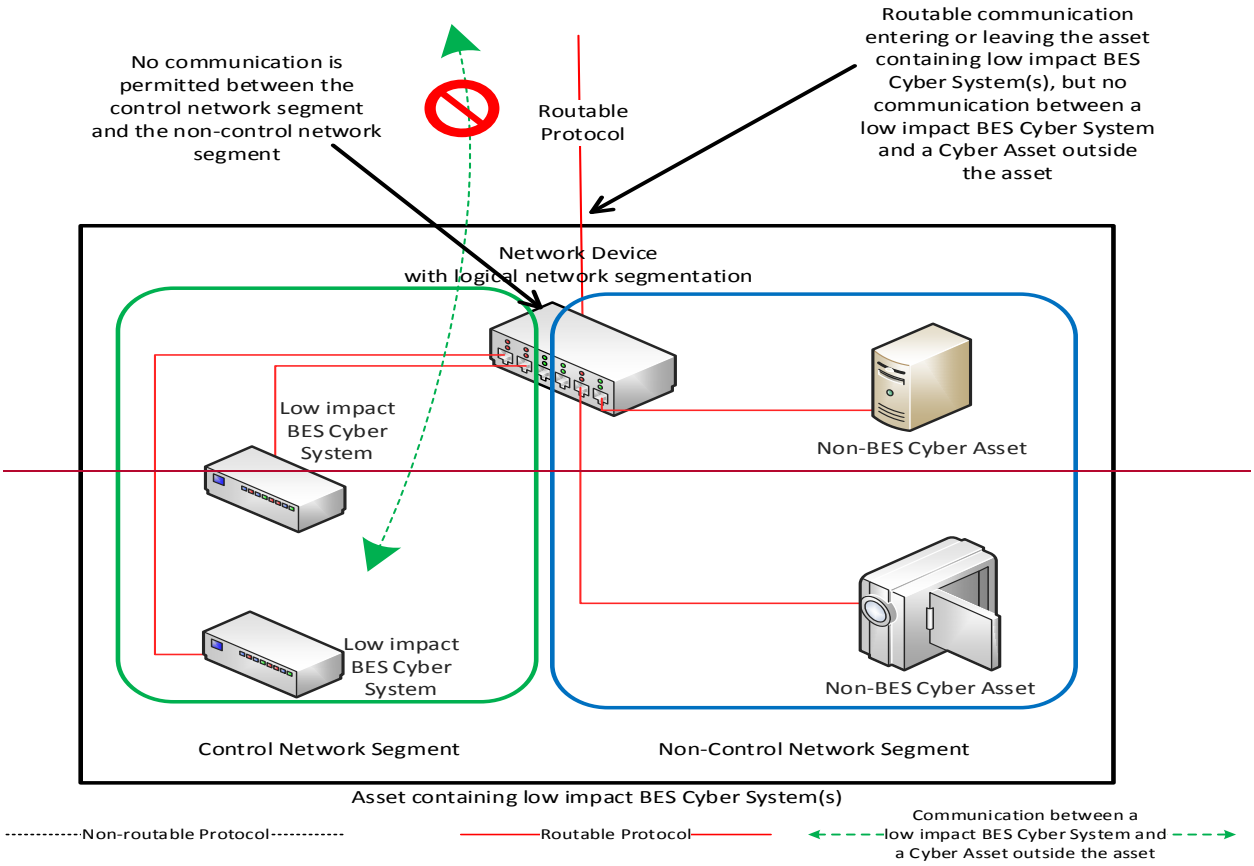
~~3)~~ The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).

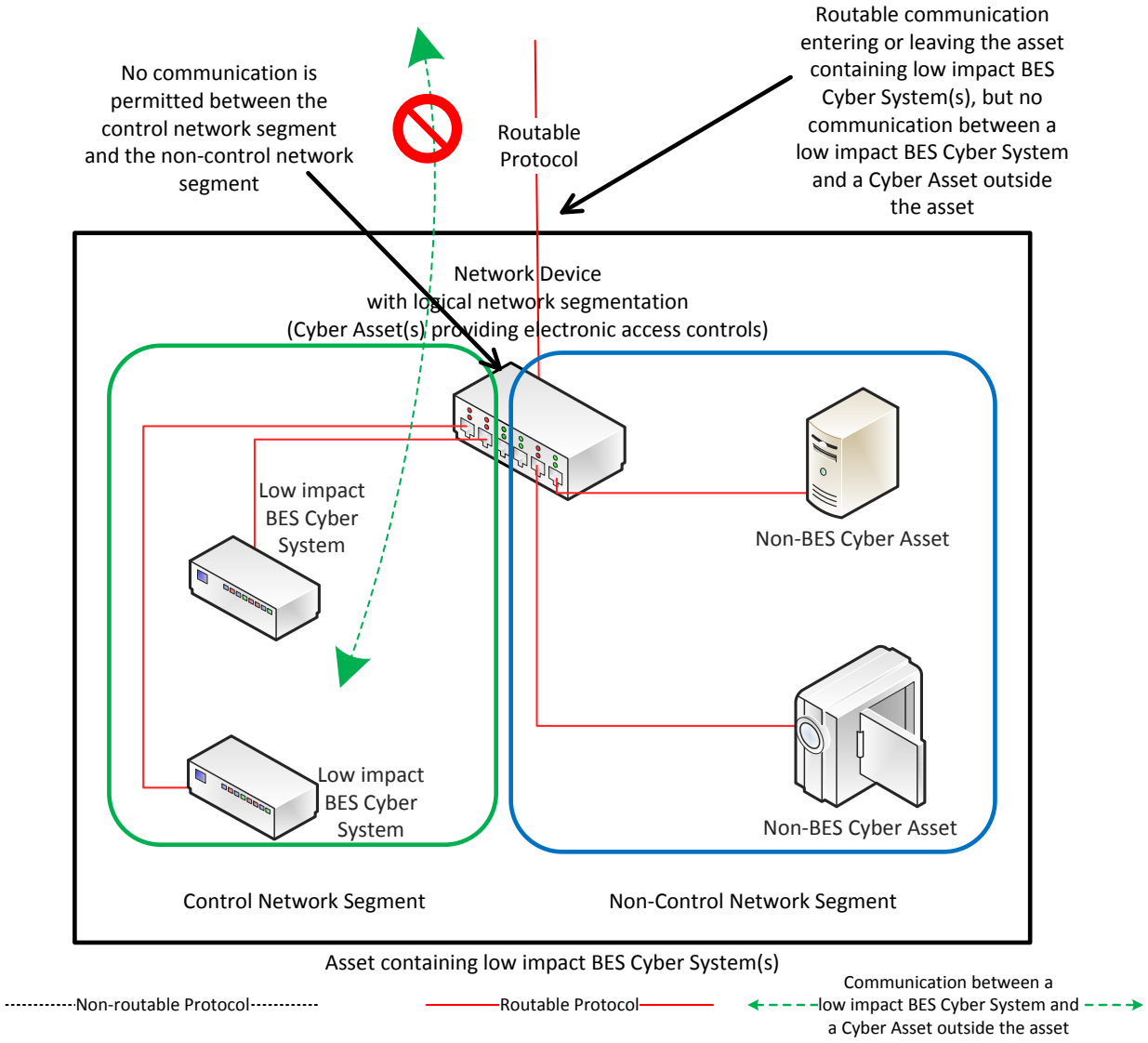


Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

In this reference model, the criteria ~~for~~from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.

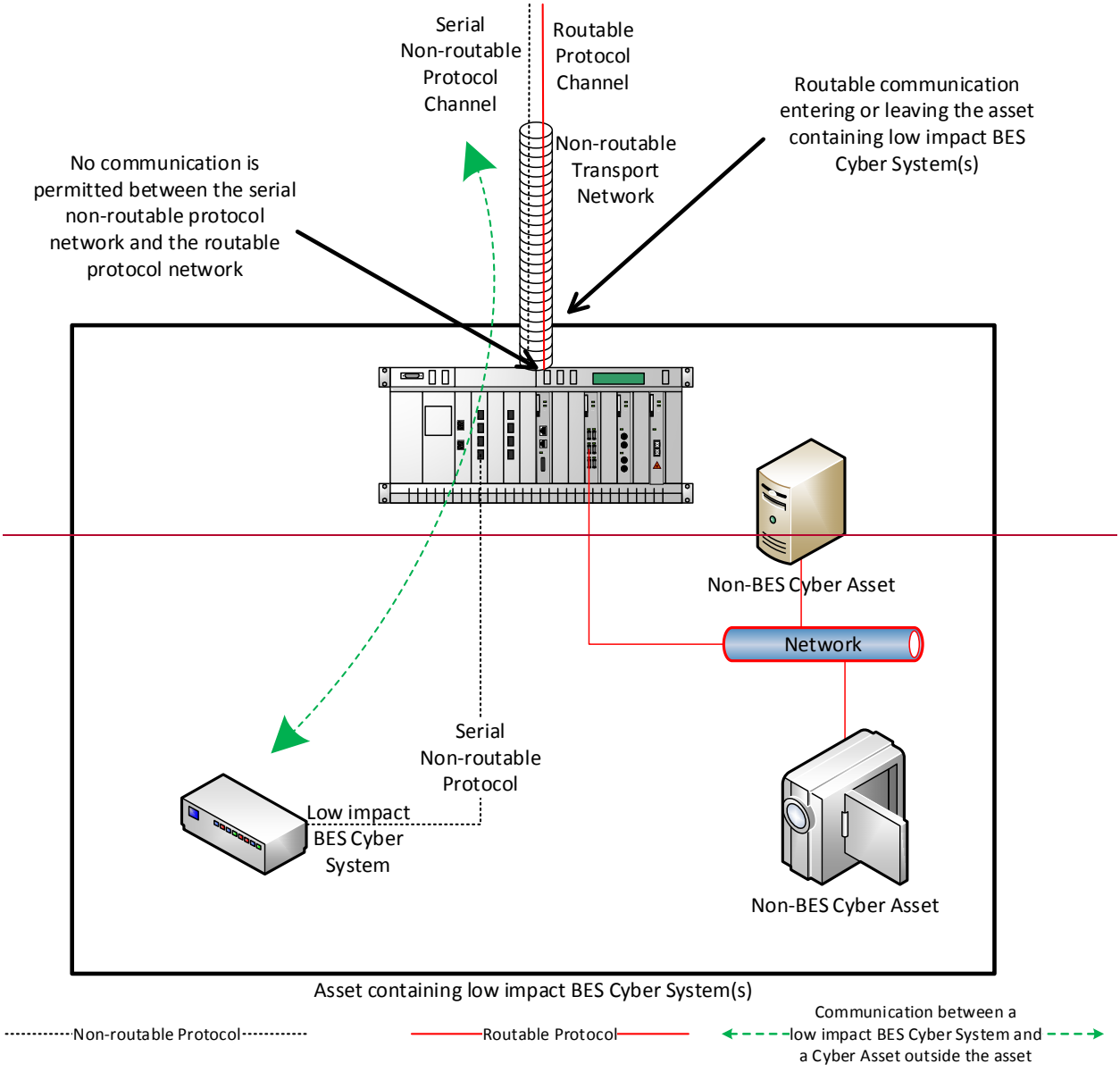


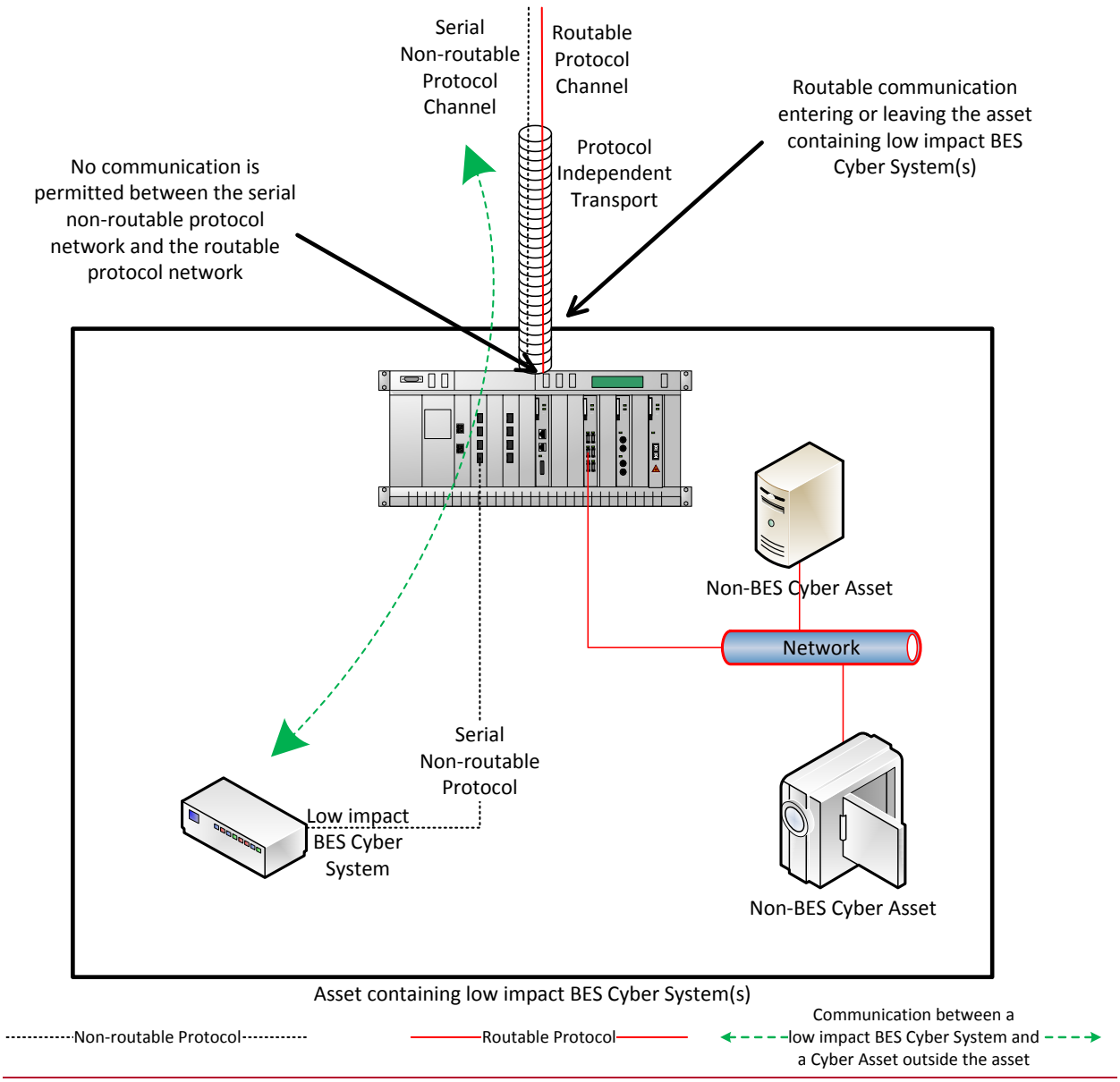


Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable ~~technology,~~communication such as a Time-Division Multiplexing (TDM) ~~or~~network, a Synchronous Optical Network (SONET~~) network. In this reference model, the criteria requiring electronic access controls are not met~~), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol. ~~In similar configurations, the Responsible Entity should closely evaluate the transport entering or leaving the asset containing low impact BES Cyber System(s). If the communication entering or leaving the asset containing low impact BES Cyber System(s) was routable (such as serial encapsulated in TCP/IP or UDP/IP as depicted Reference Model 2 or Reference Model 5), then the criteria requiring electronic access controls would be met.~~


Serial Non-routable Protocol Channel
Routable Protocol Channel
Routable communication entering or leaving the asset containing low impact BES Cyber System(s)
Non-routable Transport Network
No communication is permitted between the serial non-routable protocol network and the routable protocol network
Non-BES Cyber Asset
Network
Serial Non-routable Protocol
Low impact BES Cyber System
Non-BES Cyber Asset
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-003-TCA Security Management Controls
(Transient Cyber Assets used at low impact BES Cyber Systems)

Requested Approvals

- Reliability Standard CIP-003-TCA – Cyber Security – Security Management Controls
- Definition of Transient Cyber Asset (TCA)

Requested Retirements

- Reliability Standard CIP-003-6 – Cyber Security – Security Management Controls
- Definition of Transient Cyber Asset (TCA)

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards,* approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions. In addition to approving the seven CIP Reliability Standards, the Commission, among other things, directed NERC to "…develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems…". The Commission stated:

> 32. After consideration of the comments received on this issue, we conclude that the adoption of controls for transient devices used at Low Impact BES Cyber Systems, including Low Impact Control Centers, will provide an important enhancement to the security posture of the bulk electric system by reinforcing the defense-in-depth nature of the CIP Reliability Standards at all impact levels. Accordingly, we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns,

> the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.

General Considerations

This Implementation Plan does not modify the effective date for CIP-003-6 in the Implementation Plan associated with CIP-003-6 nor any of the phased-in compliance dates included therein.

Effective Date

The effective date for the proposed Reliability Standard and NERC Glossary term is provided below:

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-TCA shall become effective on the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-TCA shall become effective on the first day of the first calendar quarter that is twelve (12) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Planned or Unplanned Changes

Planned or Unplanned Changes Resulting in a Higher Categorization – This implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-5 titled Planned or Unplanned Changes Resulting in a Higher Categorization.[1]

Unplanned Changes Resulting in Low Impact Categorization – This implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-6 titled Unplanned Changes Resulting in Low Impact Categorization. That section provides:

> For unplanned changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

[1] Due to the length of that section, it is not reproduced herein.

Retirement Date

Reliability Standard CIP-003-6

Reliability Standard CIP-003-6 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-TCA in the particular jurisdiction in which the revised standard is becoming effective.

Current NERC Glossary of Terms Definition of TCA

The current definition of TCA shall be retired from the NERC Glossary of Terms immediately prior to the effective date of Reliability Standard CIP-003-TCA in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards Requirements for Transient Cyber Assets

Do not use this form for submitting comments. Use the electronic form to submit comments on the **Modifications to address the Federal Energy Regulatory Commission directive regarding the mandatory protection for transient devices used at Low Impact BES Cyber Systems.** The electronic form must be submitted by **8 p.m. Eastern, Friday, November 18, 2016.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Al McMeekin at (404) 446-9675.

Development Plan for LERC and TCA Modifications

The CIP Modifications Standard Drafting Team is currently addressing eight issue areas within the CIP standards including two FERC directed issue areas that directly impact the requirements for low impact BES Cyber Systems -- the Low Impact External Routable Connectivity (LERC) modifications and requirements for Transient Cyber Assets (TCAs) used at assets containing low impact BES Cyber Systems. The LERC modifications have a regulatory filing deadline of March 31, 2017. Through outreach, stakeholders have expressed a preference for the SDT to consolidate, as much as possible, proposed changes to the standards that pertain to assets containing low impact BES Cyber Systems and to do so expeditiously. The consolidation would foster stability in the low impact requirements and enable efficient implementation of the requirements which is important given the volume of in-scope assets and the work currently underway for CIP-003-6. Consequently, the SDT and NERC staff are exploring opportunities to accomplish this objective.

This informal posting of the draft CIP-003 TCA requirements is the first step in reaching that goal by providing the SDT with valuable feedback from stakeholders that will permit the SDT to discuss and make recommended revisions to the draft TCA language prior to the conclusion of the second posting and ballot of the LERC modifications (ending December 5, 2016).

The SDT is posting the draft TCA requirements for informal comment during the formal posting period of the LERC modifications. (Note: the TCA proposal uses a subset of the language from the CIP-010 TCA requirements commensurate with the risk associated at low impact. The CIP-003 language is consistent with the existing language for Medium and High Impact BES Cyber Systems to enable a common understanding of the requirements particularly for those entities implementing a plan to cover high, medium and low impact). The SDT will use the stakeholder feedback from this informal posting of the TCA revisions to determine the next steps.

Receiving thoughtful and constructive feedback from stakeholders is critical to the success of this plan. Submitting comments in advance of the deadline is welcome. The SDT thanks you for your participation.

Questions

1. If this were a formal posting, would your entity vote to approve the TCA definition, requirement language, and implementation plan as written?

   Yes:

   No:

   Comments:

2. Definition: The SDT revised the definition of Transient Cyber Asset (TCA) such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

3. Requirement R2: The SDT revised CIP-003-TCA, Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Mitigation Plan(s) to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to provide higher assurance against the propagation of malware from transient devices. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

4. Attachment 2: The SDT revised the measures language of CIP-003-TCA, Attachment 2, Section 5 to make the evidential language consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides examples of temporarily connected devices, and strategies to consider in developing the Transient Cyber Asset and Removable Media malicious code mitigation plan(s) at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

   Yes:

   No:

   Comments:

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) date for the requirements in Section 5 of Attachment 1 in CIP-003-TCA, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

   Yes:

   No:

   Comments:

7. If you have additional comments on the proposed revisions to address the FERC directive regarding TCAs for low impact BES Cyber Systems that you have **not** provided in response to the questions above, please provide them here.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2016-02 Modifications to CIP Standards

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
After consideration of the comments received on this issue, we conclude that the adoption of controls for transient devices used at Low Impact BES Cyber Systems, including Low Impact Control Centers, will provide an important enhancement to the security posture of the bulk electric system by reinforcing the defense-in-depth nature of the CIP Reliability Standards at all impact levels. Accordingly, we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.	FERC Order 822, Paragraph 32; issued January 21, 2016	The Project 2016-02 Standard Drafting Team (SDT) revised the Attachment 1 of CIP-003-TCA to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems. Attachment 1 contains and outlines the required sections of a Responsible Entity's cyber security plan(s) for its low impact BES Cyber Systems per Requirement R2. Previously, cyber security plan(s) were required to address four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. In keeping with the stakeholder approved approach to incorporate all the requirements applicable to assets containing low impact BES Cyber Systems into one standard, the SDT expanded CIP-003-6 Attachment 1 to include a fifth area: "Transient Cyber Asset and Removable Media Malicious Code Mitigation Plan(s)". Requiring the Responsible Entity to develop and implement these plans will provide higher assurance against the propagation of malware from transient devices. The plan approach for TCAs is

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		consistent with the existing requirement structure applicable to lows and accommodates the risk level of the assets. Additionally, the SDT revised the definition of a Transient Cyber Asset (TCA). The revised definition of a TCA ensures the applicability of security controls, provides clarity, and accommodates the use of the term for all impact levels: high, medium and low. The revised definition will allow entities to deploy one program to manage TCAs across multiple impact levels. The revised definition of a Transient Cyber Asset (TCA) is: A Cyber Asset that is: 1. capable of transmitting or transferring executable code; 2. not included in a BES Cyber System; 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems; and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems.

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. As proposed, Section 5 of Attachment 1 of CIP-003-TCA mandates that entities have malware protection on Transient Cyber Assets (both entity and vendor-managed) and for Removable Media. The SDT determined that it was necessary to distinguish between the specific protections for: (i) Transient Cyber Assets managed by the Responsible Entity, (ii) Transient Cyber Assets managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media. For Transient Cyber Assets managed by the Responsible Entity, Section 5 requires Responsible Entities to use one or a combination of the following methods to mitigate the introduction of malicious code: antivirus software, application whitelisting, or some other method. The SDT recognized that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices (i.e., manage in an ongoing manner) while others have a checklist for transient devices prior to connecting them to a BES Cyber System (i.e., manage in an on-demand manner). The drafting team acknowledges both methods are effective and Section 5 permits either form of management. Because of the higher

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		frequency in which these entity-managed devices are used, the controls required for these devices are more specific. For Transient Cyber Assets managed by a party other than the Responsible Entity, Section 5 requires the Responsible Entity to review and verify the malware mitigation mechanism(s) used by the third party prior to connecting the Transient Cyber Asset (per Transient Cyber Asset capability). For Removable Media, Section 5 requires entities to use methods to detect malicious code and mitigate the threat of detected malicious code prior to connecting to a low impact BES Cyber System.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 – Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of the violation risk factor (VRF) and violation severity levels (VSLs) for Requirement R2 in proposed NERC Reliability Standard CIP-003-TCA — Cyber Security — Security Management Controls. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-003-TCA, Requirement R2	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Lower was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements for low impact BES Cyber Systems. The purpose of the plan is for entities to develop an approach involving multiple procedures to address a broad subject matter. Using a plan, Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems.
FERC VRF G1 Discussion Guideline 1 - Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2 - Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement a documented cyber security plan that contains certain sections specified in Attachment 1. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security plan, the VRF is reflective of the plan as a whole. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain low impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3 - Consistency among Reliability Standards	This requirement maps from CIP-003-6, Requirement R2, which has an approved VRF of Lower; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Failure to properly implement the cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state

VRF Justifications for CIP-003-TCA, Requirement R2	
Proposed VRF	**Lower**
Guideline 4 - Consistency with NERC Definitions of VRFs	or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion Guideline 5 - Treatment of Requirements that Co-mingle More than One Obligation	The cyber security plan requirement encompasses a number of subject matter areas for low impact BES Cyber Systems. The VRF is identified at the risk level represented by all of the plan areas in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.

VSLs for CIP-003-TCA, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber	low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its	low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)	

Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to Requirement R2, Attachment 1, Section 5.3. (R2)	assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible	OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for threat of detected malicious code on	

	Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	

VSL Justifications for CIP-003-TCA, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved Requirement R2, CIP-003-6. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-003-TCA, Requirement R2	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security plan(s) but fails to address one or more of the required sections of Attachment 1. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The action of the requirement is to implement documented cyber security plan(s). Documentation of the plan(s) is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the plan in this case; as such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity implemented all the required elements of the plan. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed Definition of: "Transient Cyber Asset" (TCA)

Term: "Transient Cyber Asset" (TCA)

Revised Definition:

A Cyber Asset that is:

1. capable of transmitting or transferring executable code;
2. not included in a BES Cyber System;
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems; and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or
   - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Redline Definition:

A Cyber Asset that is:

1. capable of transmitting or transferring executable code;
2. not included in a BES Cyber System;
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems; and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or
   - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Currently Approved Definition of "Transient Cyber Asset" (TCA):

A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

2016-02 Modifications to CIP Standards Requirements for Transient Cyber Assets

Informal Comment Period Open through November 18, 2016

Now Available

An 18-day informal comment period for the **modifications to address the FERC directive regarding the mandatory protection for transient devices used at Low Impact BES Cyber Systems** is open through **8 p.m. Eastern, Friday, November 18, 2016.**

Commenting

Use the electronic form to submit comments. If you experience any difficulties using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

Next Steps

The drafting team will review all responses received during the informal comment period and determine the next steps of the project.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Al McMeekin (via email) or at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name: 2016-02 Modifications to CIP Standards | CIP-003-TCA

Comment Period Start Date: 11/1/2016

Comment Period End Date: 11/18/2016

Associated Ballots:

There were 35 sets of responses, including comments from approximately 35 different people from approximately 35 companies representing 8 of the Industry Segments as shown in the table on the following pages.

Questions

1. If this were a formal posting, would your entity vote to approve the TCA definition, requirement language, and implementation plan as written?

2. Definition: The SDT revised the definition of Transient Cyber Asset (TCA) such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

3. Requirement R2: The SDT revised CIP-003-TCA, Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Mitigation Plan(s) to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to provide higher assurance against the propagation of malware from transient devices. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

4. Attachment 2: The SDT revised the measures language of CIP-003-TCA, Attachment 2, Section 5 to make the evidential language consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides examples of temporarily connected devices, and strategies to consider in developing the Transient Cyber Asset and Removable Media malicious code mitigation plan(s) at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) date for the requirements in Section 5 of Attachment 1 in CIP-003-TCA, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

7. If you have additional comments on the proposed revisions to address the FERC directive regarding TCAs for low impact BES Cyber Systems that you have not provided in response to the questions above, please provide them here.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
ACES Power Marketing	Ben Engelby	6		ACES Standards Collaborators - CIP	Mike Brytowski	Great River Energy	1,3,5,6	MRO
					Ginger Mercier	Prairie Power, Inc.	3	SERC
					Tara Lightner	Sunflower Electric Power Corporation	1	SPP RE
					Shari Heino	Brazos Electric Power Cooperative, Inc.	1,5	Texas RE
					Bill Watson	Old Dominion Electric Cooperative	3,4	RF
					Cassie Williams	Golden Spread Electric Cooperative	3,5	SPP RE
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					Ryan Strom	Buckeye Power, Inc.	3,4,5	RF
					Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	RF
					Eric Jensen	Arizona Electric Power Cooperative, Inc.	1	WECC
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Greg Froehling	Rayburn Country Electric Cooperative, Inc.	3	SPP RE

					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Carl Behnke	Southern Maryland Electric Cooperative	3	RF
					Susan Sosbe	Wabash Valley Power Association	3	SERC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Con Ed - Consolidated Edison Co. of New York	Dermot Smyth	3,4,5,6	NPCC	Con Edison	Dermot Smyth	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange & Rockland		NPCC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC

PPL - Louisville Gas and Electric Co.	Robert Tallman	3,5,6	RF,SERC	LG&E and KU Energy	Bob Tallman	LG&E and KU Energy	3,5,6	SERC
					Charlie Freibert	LG&E and KU Energy	3	SERC
					Dan Wilson	LG&E and KU Energy	5	SERC
					Linn Oelker	LG&E and KU Energy	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,10	NPCC	RSC	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					David Ramkalawan	Ontario Power Generation	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					MIchael Forte	Con Edison	1	NPCC

					Quintin Lee	Eversource Energy	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Sean Bodkin	Dominion	4	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Chuck Lawrence	American Transmission Company	1	MRO
					Chuck Wicklund	Otter Tail Power Company	1,5	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Shannon Weaver	Midcontinent Independent System Operator	2	MRO
					Brad Parret	Minnesota Power	1,5	MRO

					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Tony Eddleman	Nebraska Public Power District	1,3,5	MRO
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Tony Eddleman	Nebraska Public Power District	1,3,5	MRO
					Steve Keller	Southwest Power Pool Inc	2	SPP RE
Midcontinent ISO, Inc.	Terry Bllke	2		IRC-SRC	Christina Bigelow	ERCOT	2	Texas RE
					Kathleen Goodman	ISONE	2	NPCC
					Ben Li	IESO	2	NPCC
					Terry Bilke	MISO	2	RF
					Greg Campoli	NYISO	2	NPCC
					Mark Holman	PJM	2	RF
					Charles Yeung	SPP	2	SPP RE
Oxy - Occidental Chemical	Venona Greaff	7		Oxy	Venona Greaff	Occidental Chemical Corporation	7	SERC
					Michelle D'Antuono	Ingleside Cogeneration LP.	5	Texas RE

1. If this were a formal posting, would your entity vote to approve the TCA definition, requirement language, and implementation plan as written?

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
See question 3 comments for our explaination.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
We suggest the drafting team include the approval of the RSAW into the Implementation Plan as this is a significant and related document. Also, we have a concern pertaining to the background information in the Implementation Plan (page 1) in reference to the terms “Low Impact BES Cyber Systems” and Low Impact Control Centers.” The FERC Order 822 language mentions both terms, and both are capitalized; however, nether term is defined in the NERC Glossary of Terms. Additionally, in the Standard, the lower case term “low impact BES Cyber Systems” is used throughout the document. If these terms are defined in a particular Standard, we suggest adding these terms to the Glossary of Terms; if not, confusion and the appearance of inconsistency in the Standard Development Process may result. Additionally, we are concerned about tracking TCAs, and the protections surrounding the various TCAs, that are being connected to the Low Impact. From a Cyber Security perspective, utilization of the cleanest possible computers makes sense; however, from a risk perspective, low impact BES Cyber Systems are, by definition, low risk. Mandating TCAs for low impact Cyber Systems will result in additional costs to utilities without clear justification of the risk. Ultimately, the TCA requirements are more stringent than the requirements for low impact Cyber Systems. We would recommend that the utilities use their business computers to connect to the cyber system.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No

Document Name	
Comment	
We believe the SDT should consider these comments before continuing with a formal posting.	
Likes 0	
Dislikes 0	
Response	
Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP	
Answer	No
Document Name	
Comment	
We would not support the requirement language that is proposed for Transient Cyber Assets (TCA), as this revision introduces controls that are similar to controls that would be written for medium impact BES Cyber Systems. There needs to be differentiation between a low impact and medium impact requirement, as this proposal blurs the line between the two impact levels.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	No
Document Name	
Comment	
See comments below.	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	No
Document Name	

Comment	
LG&E and KU Energy’s concern with certain wording in the Guildelines and Techinal basis are addressed in the response to Question 5 below.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	No
Document Name	
Comment	
In general, this okay. Please add to Attachment 2, Section 5: “A log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset is not required.” Reason: This is parallel to and in line with the specific statement in CIP-002 and CIP-003 that “an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.”	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
The redlines to the TCA definition do not substantively improve the TCA definition.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	
Answer	No
Document Name	
Comment	

The new definition does not explicitly state where it applies to Low Impact BES Cyber Systems, including Low Impact Control Centers as requested in Order No. 822. The definition should not limit the time of connection to 30 days since some diagnostic tools may be connected indefinitely.

Likes 0	
Dislikes 0	

Response

Yuguang Xiao - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	Yes
Document Name	

Comment

Change answer to NO. Con Edison is supporting NPCCs comments on this question.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	Yes
Document Name	

Comment

Seminole supports the definition and anticipates voting yes based on current analysis. Seminole requests that the team consider whether a line should be added to the definition:

2.5: not an Electronic Access Control and Monitoring System (EACMS) with high or medium impact BES Cyber Systems;	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Tri-State would vote to approve the revised TCA definition and the implementation plan as currently drafted. Depending on the SDT's response to our comment on Question 4, Tri-State may have concerns with the standard draft.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
no comments	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,3,5 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Bilke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Linsey Ray - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Definition: The SDT revised the definition of Transient Cyber Asset (TCA) such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

Teresa Cantwell - Lower Colorado River Authority - 1,5,6

Answer	Yes
Document Name	

Comment

no comments

Likes 0	
Dislikes 0	

Response

Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

CenterPoint Energy supports the revised Transient Cyber Asset (TCA) definition. CenterPoint Energy recommends that the SDT also consider updating the "Removable Media" definition to align with the proposed changes to the TCA definition. CenterPoint Energy proposes the following revisions to the "Removable Media" definition to provide clarity and applicability for low, medium, and high impact BES Cyber Systems:

Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP ***containing high or medium impact BES Cyber Systems****, or a Protected Cyber Asset* ***associated with high or medium impact BES Cyber Systems****. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.*

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	Yes
Document Name	

Comment

The IRC recommends that the standard drafting team consider revising the definition of "Removable Media" so that it is consistent with the revised definition of TCA.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

The IESO recommends that the standard drafting team consider revising the definition of "Removable Media" so that it is consistent with the revised definition of TCA.

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	Yes
Document Name	

Comment

Change answer to NO. Con Edison is supporting NPCCs comments on this question.

Likes 0	
Dislikes 0	

Response

Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 3,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	
Answer	No
Document Name	
Comment	

The revised definition does not explicitly state applicability to Low Impact BES Cyber Systems including Low Impact Control Centers. Also, the definition should not limit the time of connection to 30 days since some diagnostic tools may be connected indefinitely.

If the SDT intended to include all low impact BES Cyber Assets as part of the definition, Reclamation recommends changing the definition in item four to the following:

4. temporarily directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to any:

- BES Cyber Asset associated with high, medium, or low impact BES Cyber Systems
- network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or
- PCA associated with high or medium impact BES Cyber Systems.

Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	

- Because the redlines that NERC SDT has included use “and” statements (instead of “or” statements), NRG does not agree that the redline changes effectively address the Low Impact BCS. Any transient cyber asset requirements for Low Impact BCS will increase the cyber security requirements for the Low Impact sites. The TCA definition implies that the entity would know when a TCA is connected to a low impact BES Cyber System when that BES Cyber System may not be explicitly identified.
- NRG recommends that the NERC SDT consider rewording the redline changes to the TCA definition.

Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	No
Document Name	
Comment	
We recommends No and cannot agree on alternative language that satisfies both security and compliance needs. We are not comfortable with the way the language does not address low Impact networks.	
Likes 0	
Dislikes 0	
Response	
Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP	
Answer	No
Document Name	
Comment	
We disagree with the approach taken because it is unnecessary to introduce additional requirements prior to the effect dates of low impact requirements. We strongly recommend the SDT delay any future development on low impact standards until after the effective date has passed to allow industry and the ERO Enterprise an opportunity to assess any associated risks. The FERC directive stated that NERC should develop requirements for low impact TCA “based on the risk posed to bulk electric system reliability,” and it is very difficult to assess that risk until the requirements are enforceable.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

We recommend that the SDT modify the Removable Media definition in addition to the TCA definition. Add “containing high or medium impact BES Cyber Systems” after ESP; add” associated with high or medium impact BES Cyber Systems” after Protected Cyber Asset; and add “of Removable Media” after “Examples.”

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE does not agree the changes to the proposed definition are necessary. Adding the phrase “associated with high or medium impact BES Cyber System” is redundant as PCAs inherently apply to medium and high impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Yuguang Xiao - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

See comment for Question 1.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

The current structure is confusing.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
See question 3 comments for our explaination.	
Likes 0	
Dislikes 0	
Response	

3. Requirement R2: The SDT revised CIP-003-TCA, Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Mitigation Plan(s) to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to provide higher assurance against the propagation of malware from transient devices. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	Yes
Document Name	

Comment

Answer = Yes. Con Edison is supporting NPCCs comments on this question.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

As proposed, the modifications to Section 5 “Each Responsible Entity shall implement one or more plan(s) to achieve the objective of mitigating the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media, which shall Include”. There is a concern, that if malware is introduced onto a low impact BES Cyber System from a TCA, and the malware was not prevented by the controls you implemented then this could be interpreted to be a violation The Standards Drafting Team should clarify that an introduction of malware, even when an entity has controls in place, is not a violation unless it is shown the entity did not have controls in place or the entity did not use those controls.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,3,5 - WECC

Answer	Yes
Document Name	

Comment

We would like additional clarification to help our understanding of the responsibilities of Third Pary TCA's and Removable Media Mitigation Plan(s).

Likes 0	
Dislikes 0	

Response

Matt Stryker - Georgia Transmission Corporation - 1 - SERC

Answer	Yes
Document Name	

Comment

Regarding 5.1 & 5.2: The phrase "use of one or combination of the following method," provides little direction as to the measurability of success in compliance in terms of how many methods would be acceptable.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

Exelon is in general agreement with the approach to mirror the CIP-010 language for TCAs associated with High and Medium BCSs in CIP-003-TCA for TCAs associated with Low BCSs. However, if a decision is made to revise both CIP-010 and CIP-003 language relevant to TCAs, we believe the following additional revisions should be also be made:

1. The Standard should remove the language requiring that the mitigation plans "achieve the objective of mitigating the introduction of malicious code." This suggests that any introduction of malicious code would be noncompliant because that would be a failure to "achieve the objective." The Standard should instead require the implementation of "one or more plan(s) to mitigate the introduction . . . ."

2. For 5.1, if any "other methods to mitigate the introduction of malicious code" are acceptable, the Standard should simply require that Responsible Entities implement "one or more methods to mitigate the introduction of malicious code." The examples and possibilities can be included in the GTB.

3. For 5.2, if any "other methods to mitigate the introduction of malicious code" are acceptable, the Standard should allow other parties managing such assets to implement "one of more methods to mitigate the introduction of malicious code." The examples and possibilities can be included in the GTB.

4. Provide more clarity on what the Standard means by "managed by a party other than the Responsible Entity." Attachment 1 Section 5 distinguishes between TCAs managed by the Responsible Entity and TCAs managed by a party other than the Responsible Entity. However, the Standard does not explain how to determine who "manages" a TCA. Given the various agency, vendor, and service provider relationships in the industry, the Standard

should provide specific guidance on how to determine whether a Responsible Entity or another party is “managing” a TCA. To confuse this further, the GTB refer to TCAs being under the “control” of the Responsible Entity or a third party.

4a. If a contractor is working on a temporary basis for a Responsible Entity, are any TCAs used by that contractor “managed” by the Responsible Entity? If the TCAs are provided by the temporary agency, does that change the analysis?

4b. If a TCA is used by a vendor providing services to the Responsible Entity, is that TCA “managed” by the vendor? What if the vendor has agreed to follow the Responsible Entity’s CIP compliance program?

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

Note that while the IESO agrees with the revisions we do not have any low impact assets which would be impacted therefore we would likley abstain from a vote.

Likes 0	
Dislikes 0	

Response

Terry Bilke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	Yes
Document Name	

Comment

Note that while the IRC members agree with the revisions we do not have any low impact assets which would be impacted therefore we would likley abstain from a vote.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	Yes
Document Name	
Comment	
See comments to question 2.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
no comments	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

The proposed CIP-003, Attachment 1 additions appear to provide a workable framework for meeting FERC's directive set forth in FERC Order No. 822 that the revised Standard provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk to BES reliability. Specifically, the proposed additions to CIP-003, Attachment 1 require entities to develop "and implement one or more plans to achieve the objective of mitigating the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets (TCAs) or Removable Media." Thus, although the proposed additions to CIP-003, Attachment 1 provide registered entities with broad discretion in how to develop protections for TCAs and Removable Media, Texas RE interprets the proposed additions to CIP-003, Attachment 1 as appropriately requiring entities to: (1) develop procedures to achieve the obligation of mitigating the introduction of malicious code to low impact BES Cyber Systems; and (2) implement those procedures to achieve that objective. That is to say, the proposed additions appropriately reflect a results-based approach that provides flexibility in achieving the reliability goal, but at the same time requires the elected methods to actually work to mitigate the introduction of malicious code.

Texas RE recommends including the same criteria for low BES Cyber Assets in CIP-003 as it does for medium and high BES Cyber Assets in CIP-010. The standards will be more consistent and achieve reliability objectives. Texas RE suggests including the following language from CIP-010:

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient

Cyber Asset(s), each Responsible Entity shall authorize:

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

1.2.2. Locations, either individually or by group; and

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

functions."

"3.1. Removable Media Authorization: For each individual or group of Removable

Media, each Responsible Entity shall authorize:

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

3.1.2. Locations, either individually or by group."

Texas RE recommends making the following grammatical changes to the attachment language:

- Page 26, Section 5, reads "*shall implement one or more plan(s)*", it should read "*shall implement one or more documented plan(s)*", to stay consistent with the other CIP Standard language, which requires entities to have documented plans.
- Page 26, Section 5.1, reads: "*For Transient Cyber Asset(s) managed by the Responsible Entity, if any, use of one or a combination*". The term "of" should be removed.
- Page 29, Section 5, #2 - there should be a period (.) after "…capability".

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The SDT has clearly defined Transient Cyber Asset which in essesence is a physical object that can be connected to **or** something that has the ability to transmit executable code to BES Cyber Asset, to a network within an ESP or PCA. The second part of Section 5, deals with Removable Media Malicious Code Mitigation Plan(s). Removable Media is defined as any storage device that can be removed from a computer while the system is running, i.e., CDs, USB drive, etc. The Removeable Media **is** the Transient Cyber Asset per the proposed definition. What we need to accomplish is to assure that Malicious Code is not introduced into a BES CA, ESP or PCA via a Transient Cyber Asset and be within a plan that describes how we will prevent this.

The current wording for Transient Cyber Asset and Removable Media Malicious Code Mitigation Plan(s) is confusing to entities since it has too many objectives within one sentenance. The NSRF recommends the following;

1. Section 5 should be rewritten to reflect "Transient Cyber Asset and malicious code mitigation Plan(s)".

2. Update the Rational box (or Guidelines and Technical basis) to explain that Removable Media is defined as any "storage device that can be removed from a computer while the system is running, i.e., CDs, USB drive, etc."

3. Since Removable Media is a TCA, remove "Removable Media" within the sub sections of Section 5.

If this proposition does not work for the SDT, then it is recommended the following be rewritten:

1. “Transient Cyber Asset and removable media: Malicious code mitigation Plan(s)”.

2. In order to be in line with NERC’s word defining process, either define Removable Media and Malicious Code Mitigation Plans or remove the capitalization either or both (as above).

Section 5, we do not know the difference of 5.1 and 5.3 when a TCA is removable media? This causes confusion without definitions as requested, above. Part 5.1 first bullet says the same thing as 5.3.1: to detect malicious code.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

This is too complicated and overburdensome. Our understanding is that Section 5 lays out a considerable regulatory scheme for cyber assets that are one step removed from cyber assets that are by definition low risk and unlikely to impact reliability of the BES.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

Seminole appreciates the effort by the standard team to develop this draft update to CIP-003 and to provide a process consistent with those for medium and high impact Cyber Assets.

Section 4.2 of the standard specifically states:

“Facilities: …the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable…

Whereas the attachment 1 section 5.2 states:

For Transient Cyber Asset(s) managed by a party other than the Responsible Entity…

As the owner of the cyber asset not managed by the entity may also not be owned by the entity, the Transient Cyber Asset may be outside the scope of the requirement. Note this same issue is also present in the current version of CIP-010. Clarity needs to be provided regarding this issue.

There is significant ambiguity In the Guidelines and Technical Basis Section of the document related to systems with built-in protection capabilities. Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity, Seminole recommends adding the following language:

Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed <<or by documenting the built-in capabilities present and used on the Cyber Asset that prevents introduction of malicious code>>.

Seminole also recommends the use of tables such as those used in most of the other CIP standards that indicate applicability, requirement, and measure as this is a more effective method of communicating the requirement and expected evidence to the entity.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6

Answer	No
Document Name	

Comment

Dominion finds the wording in Section 5.3.2, “prior to connecting” is somewhat confusing. Similar wording in CIP-010 has been interpreted to mean that removable media must be re-checked whenever it is taken to a new BCS. In the situation where a single removable media is carried to multiple substations where each substation has one or more BCS. The removeable media is not inserted into anything other than the substation BCS. In this situation, the removable media is unlikely to become infected within the substations. Dominion recommends the SDT consider this scenario in a possible revision to the requirements to scan and mitigate prior to the initial connection to a BCS and after subsequent connections to non-BCS cyber assets capable of installing malware to the removable media. Dominion proposes the following language for Attachment 1, Section 5:

5.3 For Removable Media, prior to the initial introduction to a BCS and subsequent to connecting to any non-BCS cyber asset capable of installing malware to the removable media, and prior to connecting to a BCS perform each of the following:

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

5.3.2 Mitigate the threat of detected malicious code on the Removable Media.

Likes 0	
Dislikes 0	

Response

Yuguang Xiao - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	

Section 5.1: The phrase "… if any,.." is not required and should be removed. It is not clear if the phrase refers to the Transient Cyber Asset or the Responsible Entity.

Section 5.2: The phrase "… if any,.." is not required and should be removed. It is not clear if the phrase refers to the Transient Cyber Asset, the Responsible Entity, or “a party other”.

Review should also include acceptance by the Responsible Entity as indicated in the examples of evidence.

The phrase ".. live operating system and software executable only" is unclear.

Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	

The phrase “ongoing or on-demand ” adds the implication Transient Cyber Asset(s) be tracked or evidence of compliance is required, which goes beyond the other requirements for assets containing low impact BES Cyber Systems, and may not be commensurate with the risk. The other two (2) controls based sections in CIP-003-7 Attachment 1 for low impact BES Cyber Systems simply require entities to have a plan and implementation based on need, with no real evidentiary audit trail requirement of performance.

Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	

Comment
We disagree with current proposed language in Section 5.1. We assume that various members of staff will have accesss to and use of this particular asset. We suggest adding language that will help mirror the review level of the internal process (similar to section 5.2). If the assets and software are not thoroughly reviewed internally (by the Responsible Entity), the same potential issues would apply here as they would in section 5.2 (received data from external entitity).

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment
CIP-010-2 Requirement R4 includes “except under CIP Exceptional Circumstances,” we recommend that the SDT consider incorporating this exception for Transient Cyber Assets and Removable Media for low impact BES Cyber Systems as well. In Attachment 1, Section 5, the SDT can add this exception after “implement” and before “one or more plan(s)” to be consistent with the High and Medium requirements. Also, even though we realize the Section 5 language comes from the CIP-010-2 language, specifically “to achieve the objective of mitigating the introduction of malicious code”; however, this language can be improved upon by adding what the section is seeking to mitigate, i.e., the risk of the introduction of malicious code. We recommend changing the language to read “to achieve the objective of mitigating the risk of the introduction of malicious code…” Section 5.2 will have an impact on existing third party agreements (i.e., contracts), given the large number of low impact assets, renegotiating these contracts will be difficult. We recommend that the SDT consider adding forward-looking language or use of the CIP Exceptional Circumstances language to avoid requiring that entities re-negotiate contracts related to TCAs managed by other parties. Another possibility is to address this issue in the implementation plan, allowing sufficient time (e.g., 2 years from the FERC approval date) for entities to re-negotiate or modify their third party contracts.

Likes 0	
Dislikes 0	

Response

Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP

Answer	No
Document Name	

Comment

We do not support the changes to Attachment 1, Section 5. This section creates medium impact requirements for low impact systems, which is not commensurate with the risk. Smaller entities would bear an unnecessary risk of compliance by requiring medium impact controls. The purpose of creating three separate CIP impact levels was to require security controls based on risk. The low impact systems should not be required to have the same controls as the medium impact systems for TCA.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

- It is difficult to manage the potential spaghetti effect of these standards. In the case of Low Impact BCS - You would need to have an inventory of devices that would allow plugging in a transient device (i.e. like a laptop). The proposed definition assumes that you know down to an Asset level and the definition implies that the entity would know when a TCA is connected to a low impact BES Cyber System when that BES Cyber System may not be explicitly identified.
- NRG proposes that NERC SDT place this language in the appropriate section of CIP-010.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5 - WECC

Answer	No
Document Name	

Comment

The term “Mitigation Plan(s)” may be interpreted to refer to official enforcement actions.

Reclamation recommends the following:

- Remove the term “Plan(s)” from section 5 title in Attachment 1 and not capitalize words unless they are found in the NERC Glossary of Terms. Change Section 5 title to “Transient Cyber Assets and Removable Media malicious code mitigation.”
- Change the first sentence in section 5 to “Each Responsible Entity shall implement one or more method(s) …”
- Clarify and expand Section 5.3.1 to “use of method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System (such as a development station.)”

Likes 0	
Dislikes 0	
Response	

4. Attachment 2: The SDT revised the measures language of CIP-003-TCA, Attachment 2, Section 5 to make the evidential language consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Teresa Cantwell - Lower Colorado River Authority - 1,5,6

Answer	Yes
Document Name	

Comment

no comments

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC

Answer	Yes
Document Name	

Comment

The current format is hard to comprehend. Request re-formatting with bullets and numbers to separate the individual clauses.

Likes 0	
Dislikes 0	

Response

Terry Bilke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	Yes
Document Name	

Comment

Note that while the IRC members agree with the revisions we do not have any low impact assets which would be impacted therefore we would likley abstain from a vote.

Likes 0	
Dislikes 0	

Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Tri-State would like to get some clarification on the language "results of scan settings for Removable Media" used in Attachment 2, Section 5.3. Our understanding is that screenshots of the scan settings/code would be enough evidence to show compliance with Section 5.3.1. Is that correct or is the intention that entities must provide the results of every scan?	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Note that while the IESO agrees with the revisions we do not have any low impact assets which would be impacted therefore we would likley abstain from a vote.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
1. 5.2’s proposed methods all presume an ability to review cybersecurity practices of third parties that those third parties may consider proprietary and not open to review.	

a. The Standard should identify examples of sufficient methods that do not require access to third-party information. For example, contracts, MOUs, and other documented understandings with third-parties requiring them to implement sufficient controls should be acceptable so long as they commit to implementing those controls.

b. If the Responsible Entity's access to that third party proprietary information is subject to confidentiality limitations that prohibit disclosure to the other entities, the Standard should explain how the Responsible Entity will be able to demonstrate compliance.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	Yes
Document Name	

Comment

While Seminole supports the evidence request, Seminole would like to understand the auditor approach to this requirement part.

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	Yes
Document Name	

Comment

Answer = Yes. Con Edison is supporting NPCCs comments on this question.

Likes 0	
Dislikes 0	

Response

Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,3,5 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	
Document Name	
Comment	
In general, this okay. Please add to Attachment 2, Section 5: “A log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset is not required.” Reason: This is parallel to and in line with the specific statement in CIP-002 and CIP-003 that “an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.”	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE will continue reviewing facts and circumstances during compliance and enforcement reviews.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	
Answer	No
Document Name	
Comment	
The term “Mitigation Plan(s)” may be interpreted to refer to official enforcement actions. Reclamation recommends the following:	

- Remove the term “Plan(s)” from section 5 title in Attachment 2 and not capitalize words unless they are found in the NERC Glossary of Terms. Change Section 5 title to “Transient Cyber Assets and Removable Media malicious code mitigation.”

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

This could impact DCS upgrade or shutdowns. Requirement 5.2 is implying change control on the systems which is overly burdensome since the standards do not require an inventory on low systems.

NRG proposes that the NERC SDT place the information in Attachment 2, section 5 into bulleted format.

Likes 0	
Dislikes 0	

Response

Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP

Answer	No
Document Name	

Comment

We disagree with the proposed measures based on the same reasons we disagree with the proposed, corresponding requirements.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

See comments above.	
Likes 0	
Dislikes 0	
Response	
Yuguang Xiao - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
In bullet 3: Suggest replacing "entity" with "the Responsible Entity or the party other than the REntity" for additional clarity and consistency with previous sections.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	No
Document Name	
Comment	
Dominion recommends that Attachement 2, Section 5, Item 3, 2nd line, the word “mitigate” should be replaced with “detect”.	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	

See above. We do support having measures that are consistent with the language used in the requirements. Further, the requirements should match the glossary of terms.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Attachment 2 Section 5 states "…or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity;". This states that a vendor will have a contract with the Responsible Entity stating what they will accomplish. The SDT should know that Responsible Entities usually only write contracts for the services that a vendor will provide. This statement needs to be rewritten stating that Responsible Entities can have a contract that covers the applicable Section 5 items, thus protecting the Responsible Entity. If non-compliance was found with the Responsible Entity, then the Responsible Entity would be able to hold the vendor in contempt of contract. Note, this will be a concern on the Supply Chain Management Standard as well.

Likes 0	
Dislikes 0	

Response

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides examples of temporarily connected devices, and strategies to consider in developing the Transient Cyber Asset and Removable Media malicious code mitigation plan(s) at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	Yes
Document Name	

Comment

Answer = Yes.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,3,5 - WECC

Answer	Yes
Document Name	

Comment

Would like more clarity on Third Party GTB language that states “to the best of their capabilities” in terms of meeting the requirements. What does this mean exactly? Reference: Requirement R2, Attachment 1, Section 5.2.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

See comment 1) under Question 4 above

Likes 0	

Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Note that while the IESO agrees with the revisions we do not have any low impact assets which would be impacted therefore we would likley abstain from a vote	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	Yes
Document Name	
Comment	
Note that while the IRC members agree with the revisions we do not have any low impact assets which would be impacted therefore we would likley abstain from a vote.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
no comments	
Likes 0	
Dislikes 0	

Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	
Document Name	
Comment	

The NSRF cautions the SDT that sometimes the GTB only complicates the words of the Requirements. The SDT iknows that they cannot satisfy every Registered Entity with examples in the GTB. If the GTB is needed then perhaps the Requirements are not written clearly enough.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE inquires as to why the drafting team used the new title “Supplemental Material” rather than leaving the title as “Guidelines and Technical Basis”.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

See above. We also have concerns about how the GTB are factored into Compliance and Enforcement. In some cases it appears that they create “requirements” that must be incorporated into your program this is inconsistent with prior FERC precedent. On the other hand, it is not clear whether or not you can rely on the GTB in developing your program and ensuring compliance.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Georgia Transmission Corporation - 1 - SERC

Answer	No
Document Name	

Comment

The definition as proposed could result in a cyber asset unintentionally satisfying the four criteria for inclusion as a TCA.

Consider the example of a Non-BES distribution relay which is serially connected to a RTU which is a low impact BES Cyber System. If the non-BES protective relay should fail and be removed prior to the 30th consecutive calendar day after installation then it has satisfied the four parts of the definition and would be considered a Transient Cyber Asset.

The Standard Drafting Team should consider adding guidance to clarify the "intent" of a device as being a part of satisfying the definition of a TCA.

Likes 0	
Dislikes 0	

Response

Yuguang Xiao - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Requirement 1: "… four subject matter areas …" need to be updated to "… five subject matter areas…"

Requirement 2: "… four subject matter areas …" need to be updated to "… five subject matter areas…"

Rationale for Requirement 2: "… four subject matter areas …" need to be updated to "… five subject matter areas…"

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The information in the GTB section does not appear to be consistent with the information in Requirement R2. Our interpretation of Requirement R2 of the TCA suggests that there is not enough clarity in the Requirement to differentiate whether the focus is solely CIP-002 and its attachment 1 or if focus is the informationlocated in the document for review. We suggest adding clarity to either the Requirment or the GTB to ensure that there is no confusion as to the Requirement's intent is as well as what an audit team's interpretation of the performance of an entity during the auditing process. For example, the language used on page 45 of the Standard: "Examples of these temporarily connected devices include, but are not limited to:

Diagnostic test equipment;

Equipment used for BES Cyber System maintenance; or

Equipment used for BES Cyber System configuration.

The attachment was created to specify the capabilities and possible security methods available

to Responsible Entities based upon asset type and ownership." This detailed language from the GTB should be consistent with the Requirement language and we feel its not in this case in reference to this particular example. Additionally, the example of the devices mentioned in the GTB are not consistent with the devices in the Requirement language. We suggest that drafting team review both sections for consistency.

Likes 0	
Dislikes 0	

Response

Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP

Answer	No
Document Name	

Comment

We would like the SDT to clarify the differences between medium impact TCA and low impact TCA. We would also like the SDT to clarify in the guidelines the differences in security controls for medium and low impact BES Cyber Systems. There are no statements regarding how risks differ between levels, or how an entity should manage these risks through security controls.

Likes 0	
Dislikes 0	

Response

Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy

Answer	No
Document Name	

Comment

On page 47 under the section *Requirement R2, Attachment 1, Section 5.2 – Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity,* LG&E and KU Energy believes the language quoted below appears to go beyond what FERC requires of Entities with respect to Supply Chain standard and vendor expectations, and creates a higher burden than that in the approved High and Medium TCA standard. LG&E and KU Energy suggest the wording below be removed or updated to align with FERC's expectations, and impose no higher level of compliance upon Registered Entities than that currently in place for both High and Medium TCAs.

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsibly Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code on Transient Cyber Assets it does not manage.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

This could impact DCS upgrade or shutdowns. Attachment 2, Section 5.2 is implying change control on the systems which is overly burdensome since the standards do not require an inventory on low systems.

NRG recommends that the NERC SDT remove the change management systems reference in Examples of evidence for section 5.2.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5 - WECC

Answer	No
Document Name	

Comment

The term “Mitigation Plan(s)” may be interpreted to refer to official enforcement actions.

Reclamation recommends the following:

- Remove the term “Plan(s)” from the title “Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Mitigation Plan(s)” and not capitalize words unless they are found in the NERC Glossary of Terms. Change Section 5 title to “Transient Cyber Assets and Removable Media malicious code mitigation.”
- Add a bullet for “Equipment used for BES Cyber Asset maintenance;” in the Examples section.
- Add a bullet for “Equipment used for BES Cyber Asset configuration;” in the Examples section.

Likes 0	
Dislikes 0	

Response

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) date for the requirements in Section 5 of Attachment 1 in CIP-003-TCA, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

Teresa Cantwell - Lower Colorado River Authority - 1,5,6

Answer	Yes
Document Name	

Comment

no comments

Likes 0	
Dislikes 0	

Response

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	Yes
Document Name	

Comment

Because of the state of flux of electronic access controls associated with Low Impact BES Cyber Systems, industry as a whole has not begun to fully address the electronic access control requirements for Low Impact BES Cyber Systems. Adding additional requirements to the current requirements, while the current requirements are still changing, makes it difficult for low impact only entities to begin their implementation. Rushing implementation simply to meet an earlier enforcement date does not allow for thoughtful developement of security measures. Ensuring a date that allows for a cohesive implementation between electronic access controls and TCA/Removable Media controls will provide a higher level of security than a piecemeal approach that could result from an implementation period that is too short.

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	Yes
Document Name	

Comment	
Change answer to NO. Con Edison is supporting NPCCs comments on this question.	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Linsey Ray - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Bilke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	
Document Name	
Comment	
None of the changes impact the IRC members either positvely or negatively so we have no opinion on the Implimentation Plan	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not necessarily object to the SDT's proposed 12-month implementation period. However, Texas RE respectfully requests that the SDT provide a basis for its decision to adopt such a 12-month compliance window, including any data it considered in determining that this was an appropriate window for affected entities to meet their compliance obligations under the revised Standards.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
None of the changes impact the IESO either positvely or negatively so we have no opinion on the Implimentation Plan.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	
Answer	No
Document Name	
Comment	
Reclamation recommends a more achievable implementation plan of 24 months from the date of FERC approval.	
Likes 0	
Dislikes 0	
Response	

Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The requirements for low impact BES Cyber Systems are currently in flux and entities will not have certainty regarding low impact requirements until they are approved by the Commission. In addition, the sheer number of assets containing low impact BES Cyber Systems is substantial. It will take entities time to implement proper controls at all the various locations. CenterPoint Energy believes it is reasonable to request additional time to implement the requirements given that the facilities are low risk to the reliability of the BES. CenterPoint Energy recommends the effective date for CIP-003-TCA revisions to align with the LERC modifications.	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
NRG recommends that the NERC SDT revise the effective compliance date for the requirements in Section 5 of Attachment 1 in CIP-003-TCA to be 18 calendar months after the effective date of the applicable governmental authority's order approving the standatd and NERC Glossary term: to account for budgeting cycles.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	No
Document Name	
Comment	
Due to budget cycles and quantity of equipment that must be installed, we propose keeping the language in the "General Consideration" section but extend the interval from 12 months to 18 months.	
Likes 0	
Dislikes 0	

Response	
Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP	
Answer	No
Document Name	
Comment	
The implementation plan for TCA should not occur until 2019. We do not support the target date of September 1, 2018 because there are several other requirements that need to be met. The burden of compliance with this proposal would add significant resources and costs with implementing these low impact security measures. The implementation plan should allow for an additional budgeting cycle to ensure industry has time to implement such controls.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Although it would be helpful to implement all of the CIP-003-7 modifications at the same time, the issues we raise in the other comments should be addressed before this implementation plan is approved.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
We suggest that the effective date be moved to eighteen (18) calendar months due to the various complexities and the scope of the process.	
Likes 0	
Dislikes 0	

Response	
Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	No
Document Name	
Comment	
It is our position that there should be a focus on excellence by providing the proper timeframe for proper completion of the CIP-003 TCA requirements. The timeframe provided does not provide an adequate window for budgetary cycles, process development, implementation, and training for the successful deployment of the low impact TCA. Additional time is needed to incorporate the proper training, controls, processes and internal testing of processes to ensure success in compliance.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Process development and implementation of Low BCS electronic access controls has been significantly delayed and remains contingent upon requirements finalization. Propose allowance of a minimum of 24 months from FERC approval date to compliance date for CIP-003-7 R2, Attachment 1 Sections 2 and 3 AND 5.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy disagrees with the implementation plan proposed for CIP-003-TCA, and suggests a more achievable implementation plan of 24 months from the date of FERC approval. As written, it appears that an entity will need to create an inventory of all Low BES Cyber Systems in order to ascertain whether a device that connects to a TCA is considered a “low”. It is also possible that an entity could instruct its employees/contractors to treat all devices (high, medium, or low) the same when connecting with TCA, and assume they would fall under the purview of CIP-003-TCA and perform the	

necessary work in order to maintain compliance with CIP-003-TCA. The amount of time needed for larger entities to create such an inventory, would be significant, as would the amount of time to provide training to a large number of employees/contractors in order to maintain compliance with the proposed. We do not feel that 12 months from governmental approval is an adequate amount of time to achieve compliance with the language as written currently. We recommend to the drafting team an implementation period of 24 months from FERC approval.	
Likes 0	
Dislikes 0	
Response	

7. If you have additional comments on the proposed revisions to address the FERC directive regarding TCAs for low impact BES Cyber Systems that you have not provided in response to the questions above, please provide them here.

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	
Document Name	

Comment

Please note that within the rational box for Section 5, the SDT uses “Transient devices” as did FERC in paragraph 32. Recommend that Transient device be updated to read “Transient Cyber Asset”.

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	
Document Name	

Comment

Interpretation of the Attachment 1 Section 5 requirements is that evidentiary requirements are to document and implement the plan for managing malware protection for TCA and RM that are to be connected to Low BCSs, and that maintaining evidence for each instance of review and scan logs are not required.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Georgia Transmission Corporation - 1 - SERC

Answer	
Document Name	

Comment

The Standard Drafting Team should consider updating the glossary definition of Removable Media to reflect similar low-impact language changes as those proposed to the definition of Transient Cyber Assets.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

No additional comments

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE notes some possible issues with the proposed Violation Severity Levels associated with the proposed additions to CIP-003, Attachment 1. First, the second proposed “Lower VSL” provides that “[t]he Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to Requirement R2, Attachment 1, Section 5.3.” Although it is possible to read the VSL language as referring first to general documentation for TCAs and Removable Media and then to the two specific Removable Media elements identified in Section 5.3, this connection could be made clearer. One approach would be revise the Lower VSL to read “The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the use of method(s) to detect malicious code on

Removable Media using a Cyber Asset other than a BES Cyber System or mitigation of the threat of detected malicious code on Removable Media prior to connecting Removable Media to a low impact BES Cyber System."

Second, and related to the first issue above, the initial additional "Moderate VSL" provides that the Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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." (emphasis added). However, Section 5.3 applies to Removable Media and not TCAs. As such, the reference here seems inappropriate and potentially conflicts with the "Low VSL" for documentation of Removable Media mitigation described above. Texas RE recommends that the SDT either eliminate the reference to Section 5.3 here, or develop a new "Moderate VSL" applicable to the mitigation requirements for Removable Media in Section 5.3. The Standard Drafting Team should further ensure that this approach is consistent with the "Low VSL" for Removable Media documentation as well.

Finally, while Texas RE does not necessarily object to the general VSL assignments at this time, Texas RE respectfully requests that the SDT provide a basis for its decisions to assign VSL categories to the various elements. In particular, Texas RE would like to understand the SDT's decision to assign "Low" and "Moderate" VSL categories to Removable Media and "Moderate" and "High" VSL categories to Transient Cyber Assets.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

It would be helpful if the SDT or NERC could address what is required to demonstrate compliance with the low impact requirements at shared facilities. For example, is a Memorandum of Understanding (MOU) between the Responsible Entities that have equipment in the same low impact asset sufficient or is a Joint Registration Organization or Coordinated Functional Registration needed for the low impact CIP-003-7 requirements? If an MOU is

sufficient, what details should be addressed in the MOU? For example, which tasks or requirements is each entity responsible for performing and who is responsible for potential violations of the requirements? This is currently an unresolved issue for medium impact BES Cyber Systems and will be a bigger issue for low impact assets as there are many more low impact assets. Addressing this issue for low impact assets will also require a longer implementation timeframe given the number of low impact assets.	
Likes 0	
Dislikes 0	
Response	
Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP	
Answer	
Document Name	
Comment	
We urge the SDT to stagger its posting schedule so different drafts of the CIP standards do not have overlapping deadlines to submit comments. Industry is currently focused on implementing the existing CIP V5 standards, while also paying attention to the development of these revisions. There should not be multiple deadlines assigned to this project, as this creates a strain on CIP subject matter experts to review and provide feedback on the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	

Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
CenterPoint Energy appreciates the SDT's efforts to consolidate the TCA revisions with the LERC modifications. CenterPoint Energy is in favor of filing the TCA modifications and implementation plan with the LERC modifications, if possible.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	
Answer	
Document Name	
Comment	
Reclamation recommends the following: • Changes associated with Transient Cyber Assets and Removeable Media should be integrated into future standards and should not be an intermin standard. • Existing NERC standard naming and numbering protocol continue to be followed and that this draft standard no longer be referred to as "-TCA."	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	

Document Name	
Comment	
no comments	
Likes 0	
Dislikes 0	
Response	

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.

Description of Current Draft

This draft of CIP-003-7 is addressing the directive issued by the Federal Energy Regulatory Commission (Commission) in paragraph 73 of Order No. 822 which reads:

> [T]he Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule approving revisions to the cybersecurity Critical Infrastructure Protection (CIP) standards.

In this revision, the SDT revised Sections 2 and 3 of Attachments 1 and 2 to CIP-003-7 and removed the terms Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP). The modifications incorporate concepts and select language from the LERC definition into Attachment 1, Section 3 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). The SDT simplified Section 3 of Attachment 1 to require the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii) which reads: "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The defined term LEAP is no longer necessary because the SDT changed the requirement from requiring a LEAP to requiring electronic access controls. Additionally, since the SDT is removing the term LERC, the exclusion language that was previously in the definition of LERC was integrated into the Attachment 1, Section 3.1 requirement.

Because the proposed modifications in Reliability Standard CIP-003-7 eliminate the need for the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP), NERC is requesting these terms be retired in the associated Implementation Plan.

Completed Actions	Date
Standard Authorization Request (SAR) approved	July 20, 2016
Draft 1 of CIP-003-7 posted for formal comment and initial ballot	July 21 – September 6, 2016
Draft 2 of CIP-003-7 posted for formal comment and additional ballot	October 21 – December 5, 2016
10-day final ballot	December 9-19, 2017

Anticipated Actions	Date
NERC Board of Trustees (BOT) adoption	February, 2017
Petition filed with FERC	March, 2017

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-7

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 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 SPS or RAS where the SPS or 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-003-7:

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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3 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.

4.2.3.4 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-003-7.

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single

cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls; and

1.2.4. Cyber Security Incident response

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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate

implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans	containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented	failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2)	its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification,	The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(E-ISAC) according to Requirement R2, Attachment 1, Section 4.		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but	The Responsible Entity has used delegated authority for actions where allowed by the CIP

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specific actions delegated, but 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. (R4)	specific actions delegated, but 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. (R4)	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. (R4)	Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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.	

Version	Date	Action	Change Tracking
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 devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees.	Revised to address FERC Order 822 directive regarding definition of LERC.

Attachment 1

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

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

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

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

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The

focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

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

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

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

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Attachment 2

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

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

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

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

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

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

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

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a

combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such

communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located

at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an “electronic boundary,” but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only “necessary” inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for “necessary” inbound and outbound electronic access controls may be documented within the Responsible Entity’s cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

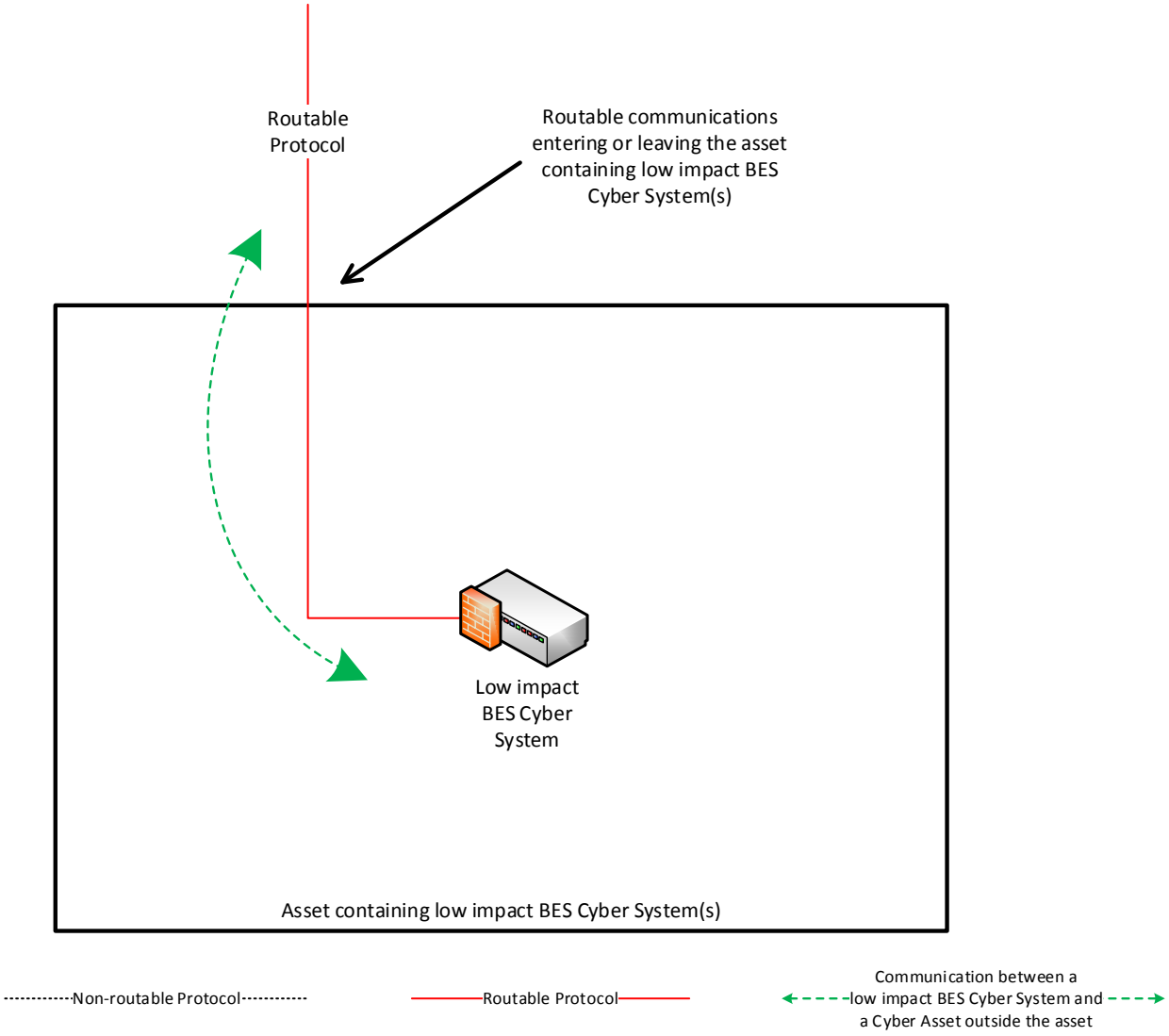
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

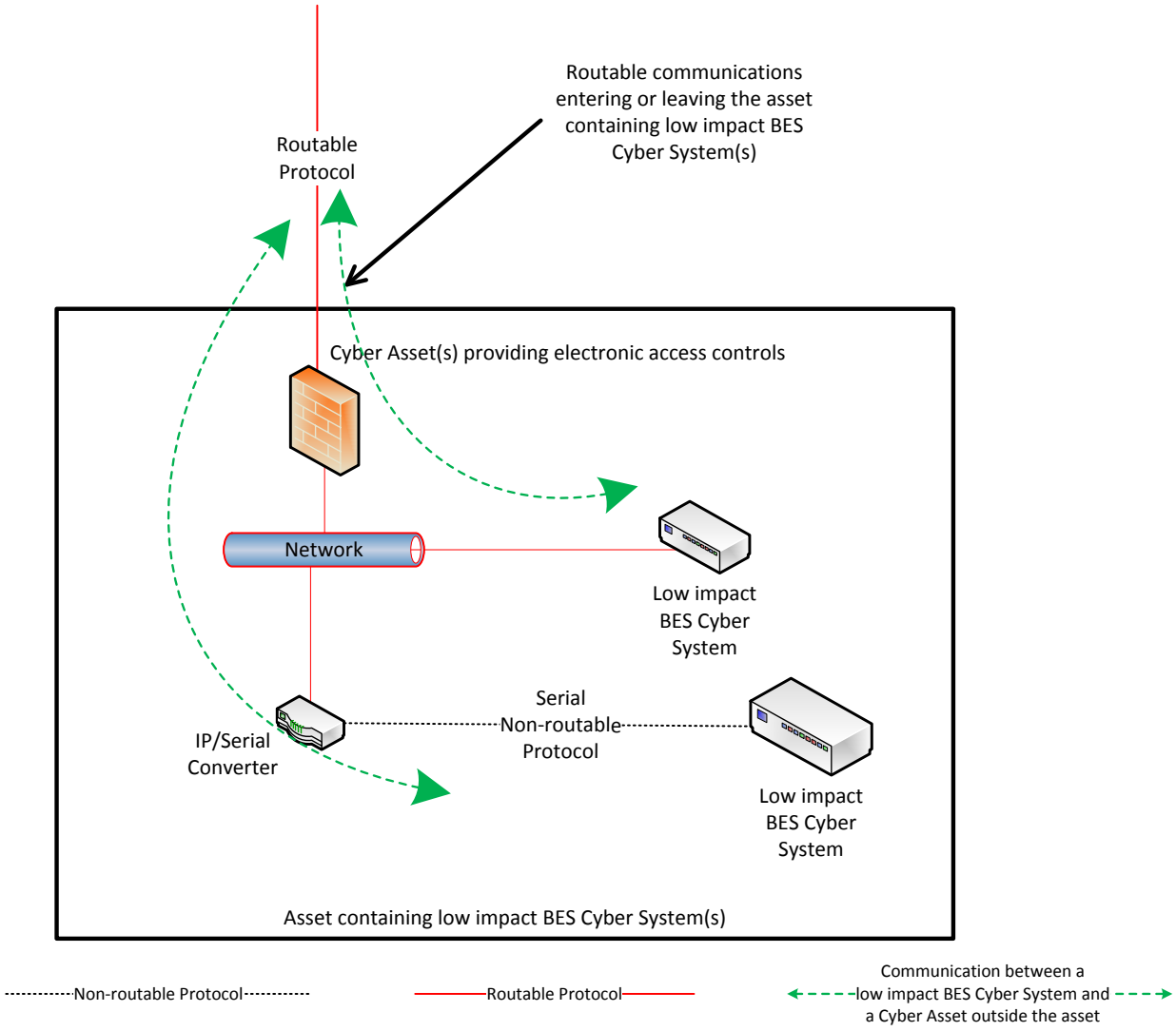
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

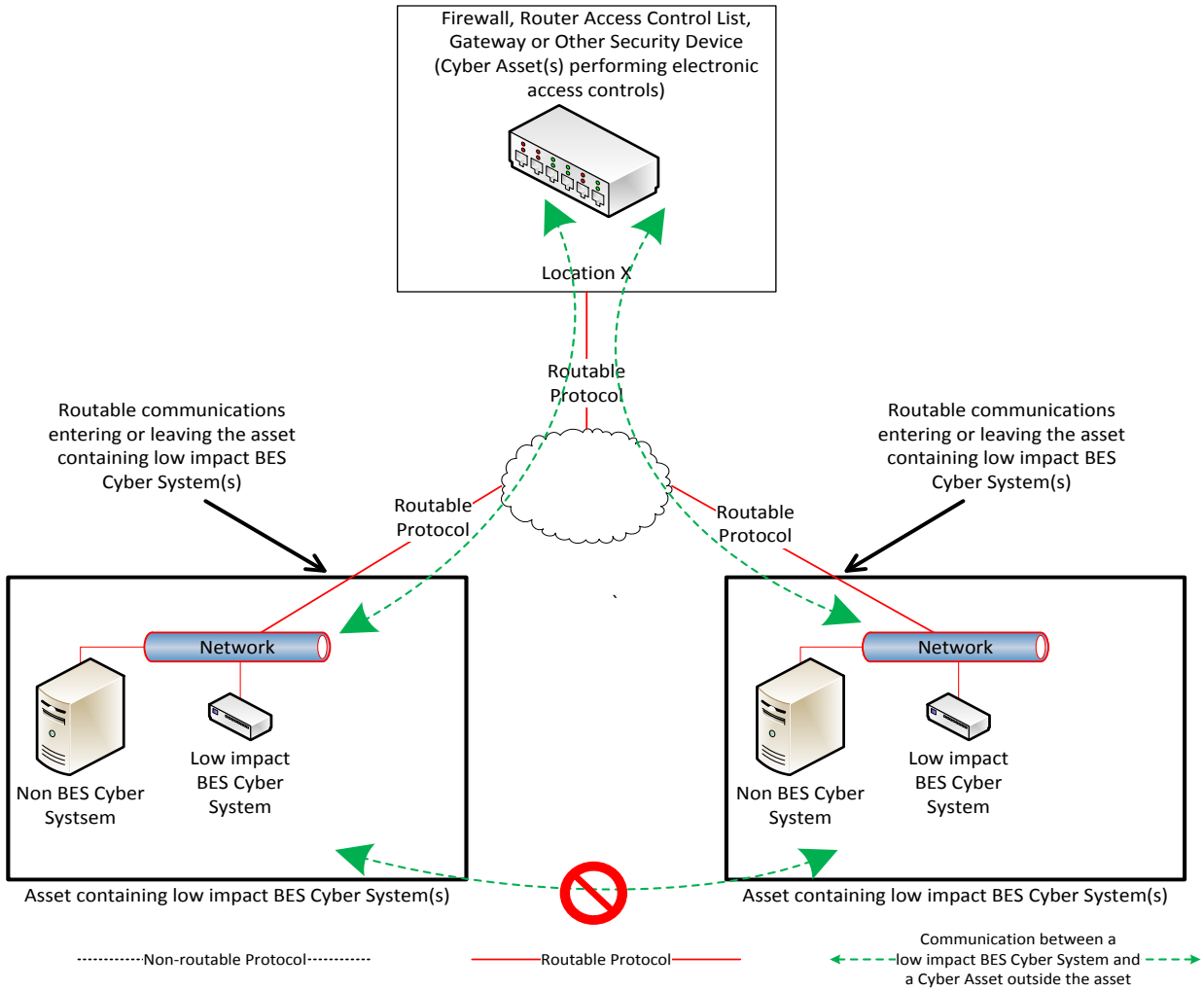
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

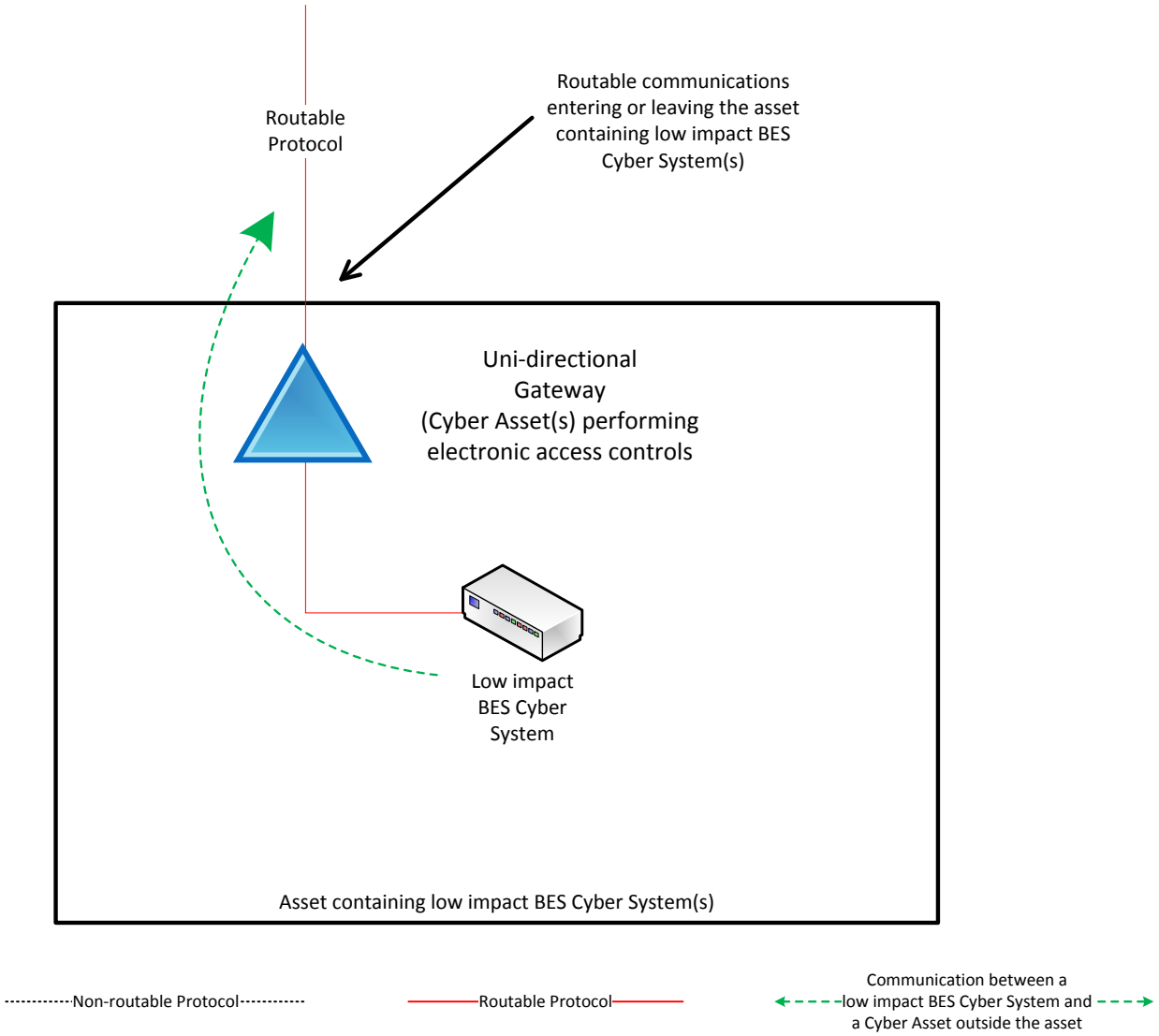
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

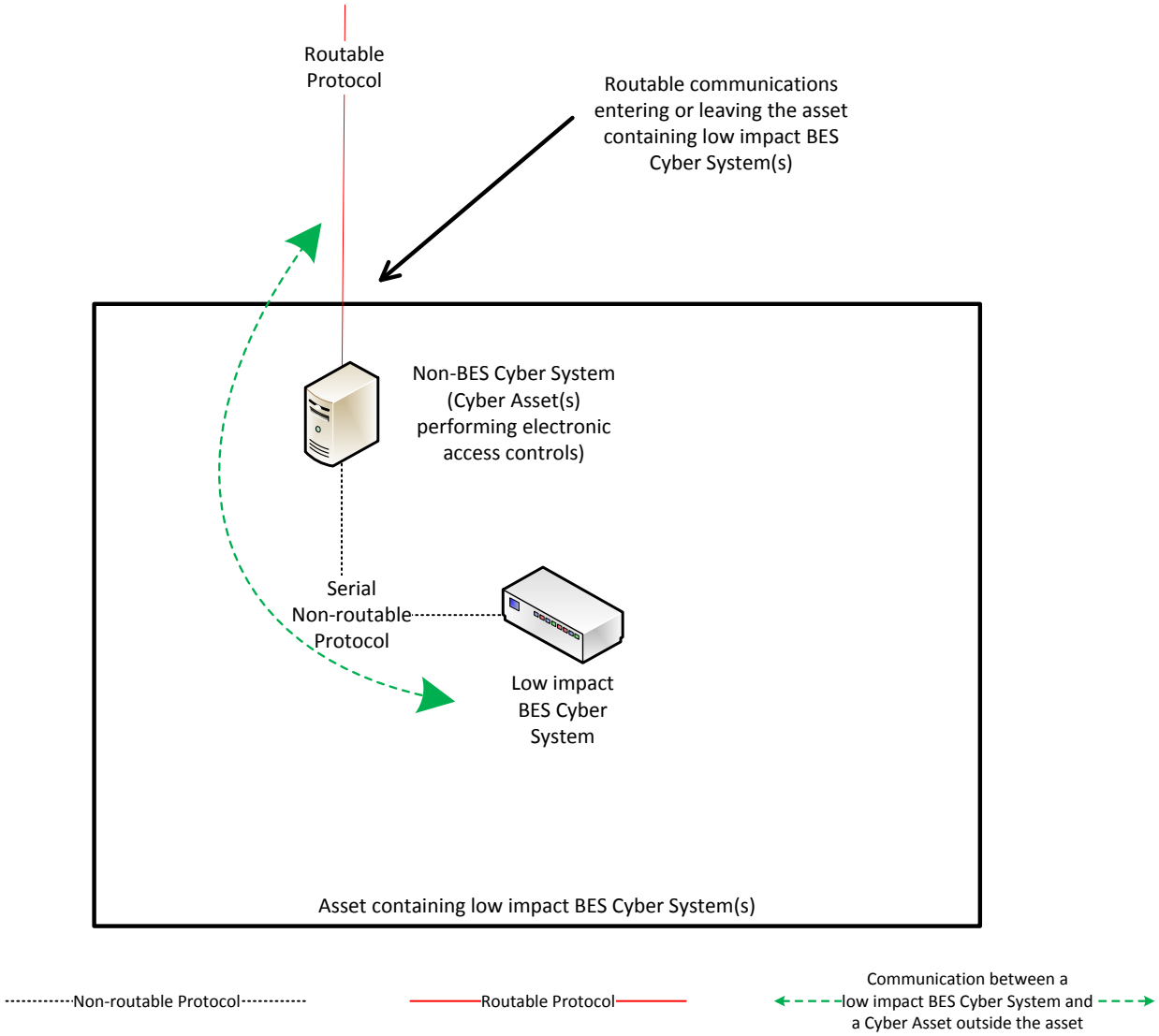
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

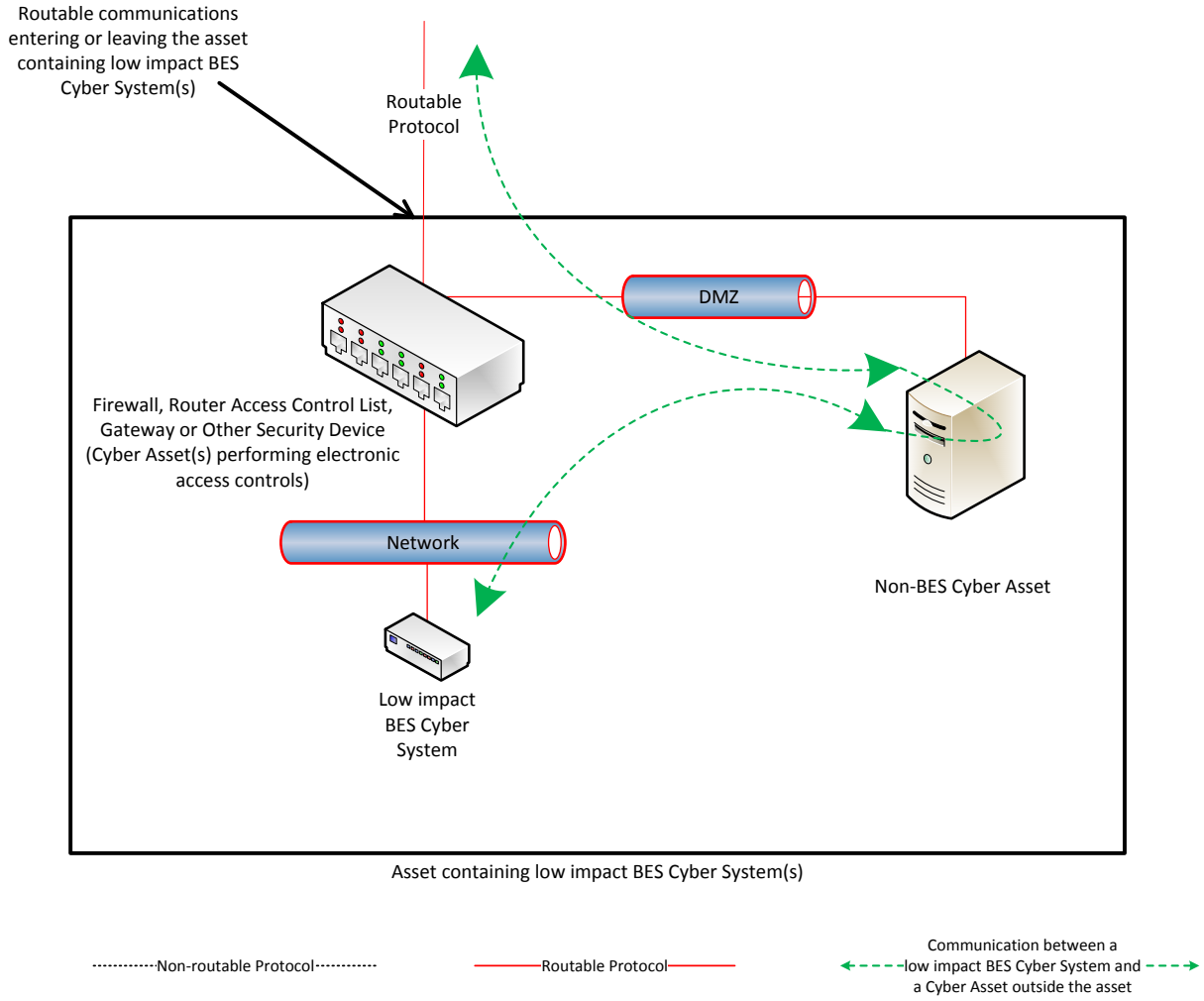
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

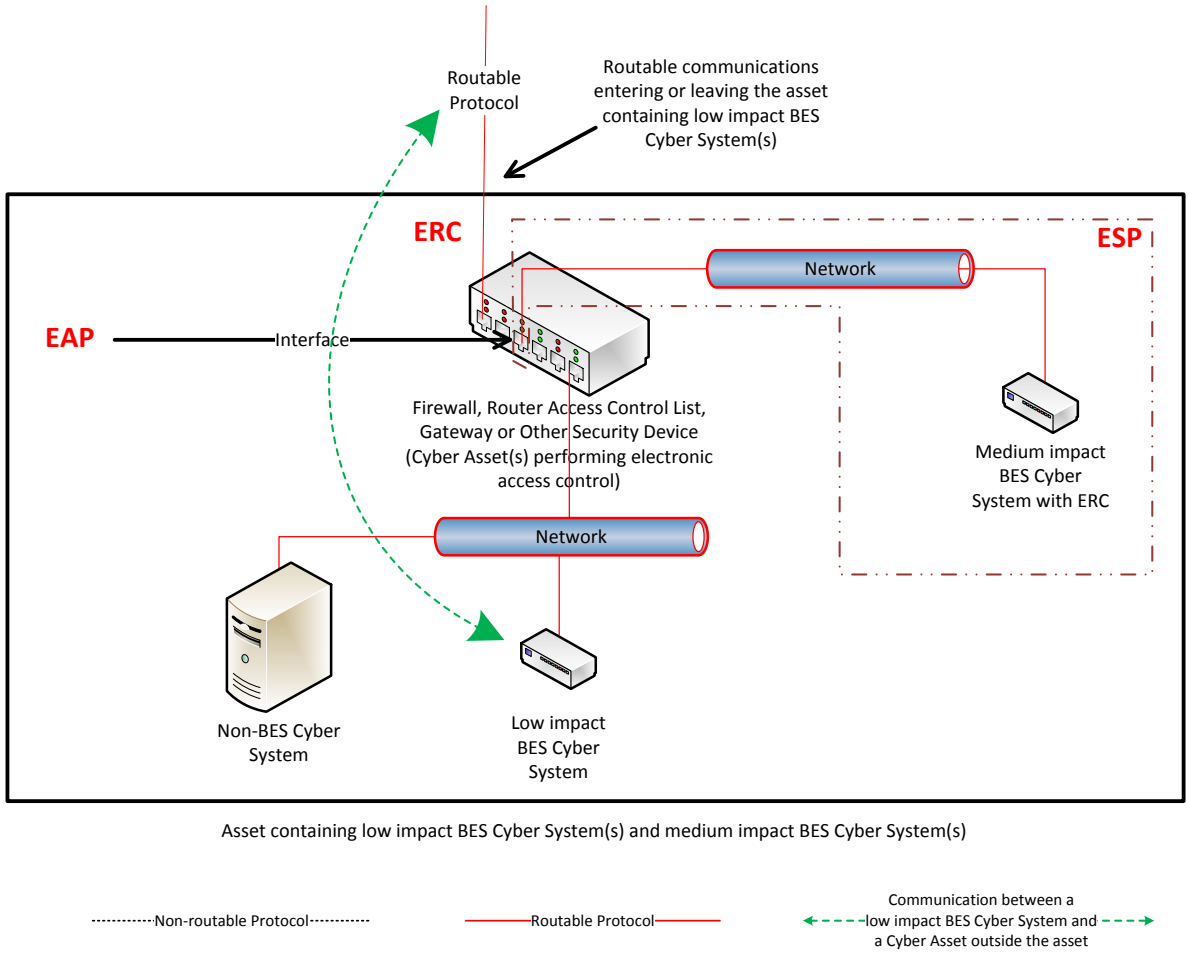
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.

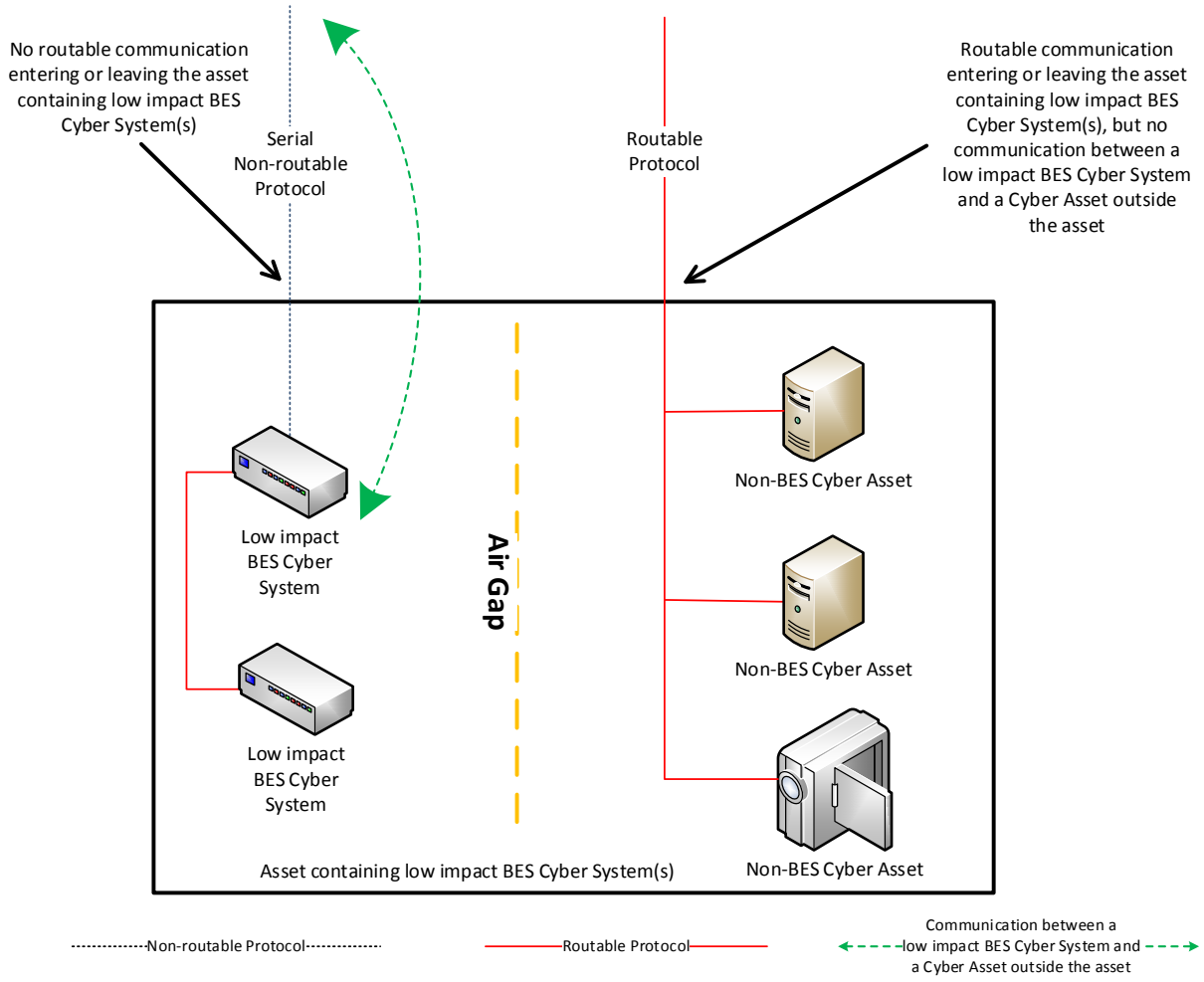


Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

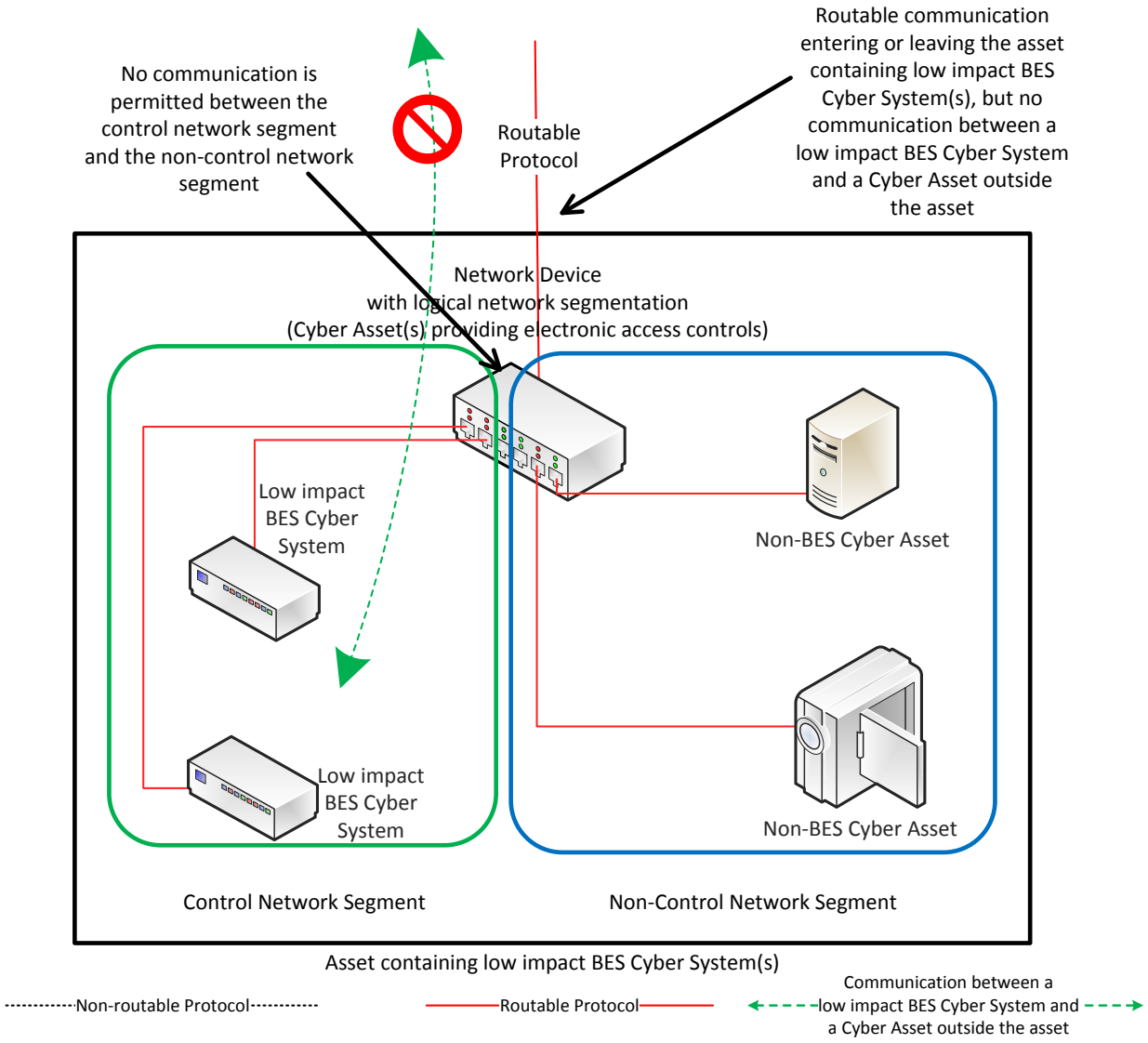
1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

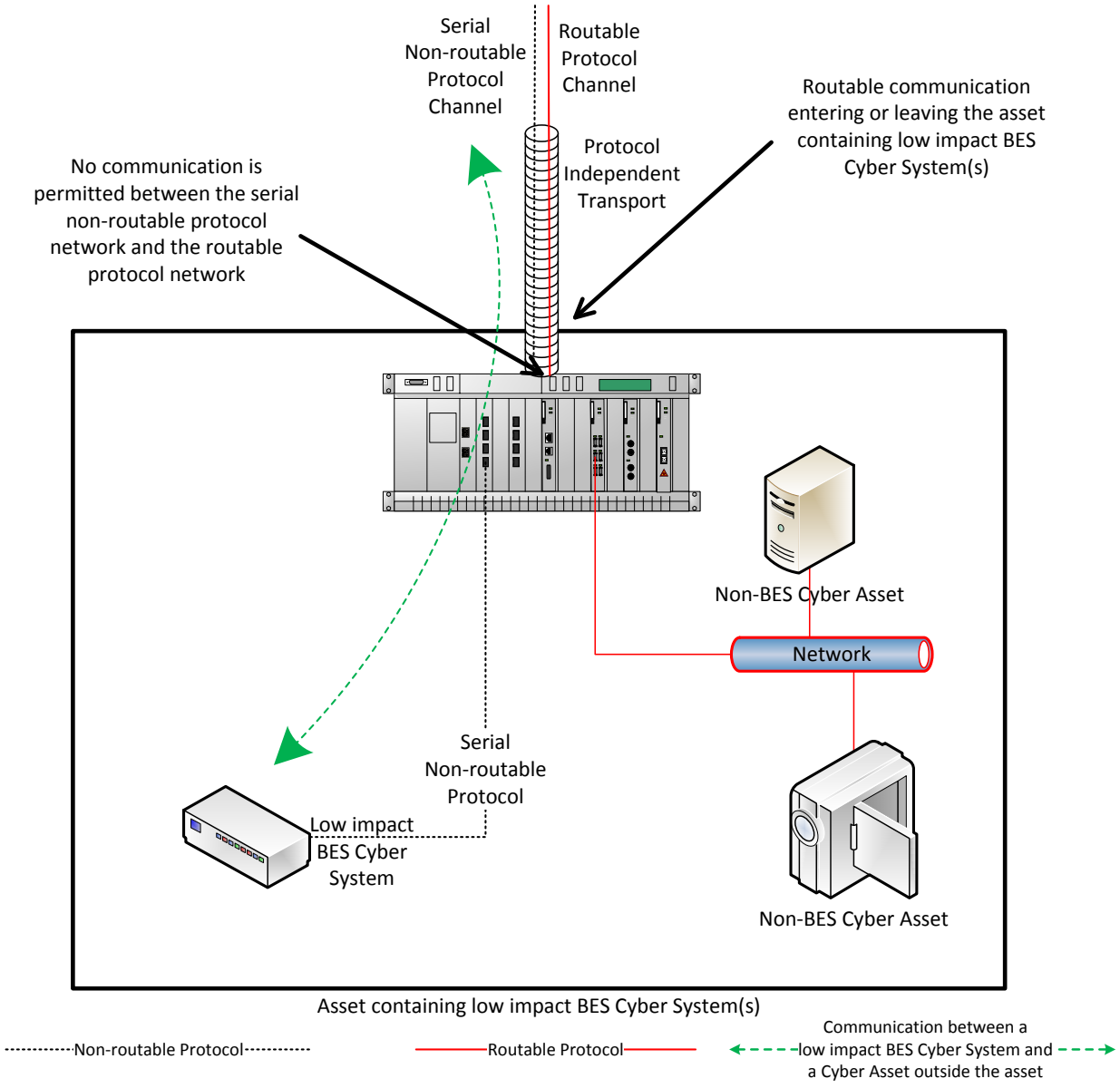
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

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.

Description of Current Draft

This draft of CIP-003-7 is addressing the directive issued by the Federal Energy Regulatory Commission (Commission) in paragraph 73 of Order No. 822 which reads:

> [T]he Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule approving revisions to the cybersecurity Critical Infrastructure Protection (CIP) standards.

In this revision, the SDT revised Sections 2 and 3 of Attachments 1 and 2 ~~in~~to CIP-003-7 and removed the terms Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP). The modifications incorporate concepts and select language from the LERC definition into Attachment 1, Section 3 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). The SDT simplified Section 3 of Attachment 1 to require the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii) which reads: "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The defined term LEAP is no longer necessary because the SDT changed the requirement from requiring a LEAP to requiring electronic access controls. Additionally, since the SDT is removing the term LERC, the exclusion language that was previously in the definition of LERC was integrated into the Attachment 1, Section 3.1 requirement.

Because the proposed modifications ~~to~~in Reliability Standard CIP-003-7 eliminate the need for the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP), NERC is requesting these terms be retired in the associated Implementation Plan.

~~Additionally, the SDT:~~

- ~~revised the associated Lower, Moderate, and High VSLs for Requirement R2 to complement the requirement revisions;~~
- ~~corrected a mistake in the Severe VSL for Requirement R2;~~
- ~~made non-substantive changes to the Moderate and High VSLs for Requirement R2 to align with the order of the requirement;~~
- ~~removed repetitive text from Requirement R1, Part 1.2.3 to make it consistent with Parts 1.2.1 and 1.2.2;~~

~~updated the Guidelines and Technical Basis section of the standard to reflect the revisions made to the Attachments; and~~

- ~~made non-substantive errata changes throughout the standard such as replacing "ES-ISAC" with "E-ISAC".~~

Completed Actions	Date
Standard Authorization Request (SAR) approved	July 20, 2016
Draft 1 of CIP-003-7 posted for formal comment and initial ballot	July 21 – September 6, 2016
Draft 2 of CIP-003-7 posted for formal comment and additional ballot	October 21 – December 5, 2016
10-day final ballot	December 9-19, 2017

Anticipated Actions	Date
~~10-day final ballot~~	~~January, 2017~~
NERC Board of Trustees (BOT) adoption	February, 2017
Petition filed with FERC	March, 2017

A. Introduction

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

2. **Number:** CIP-003-7

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 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 SPS or RAS where the SPS or 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-003-7:

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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3 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.

4.2.3.4 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-003-7.

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single

cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls; and

1.2.4. Cyber Security Incident response

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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate

implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) 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 BES Cyber Systems as	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans	containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented	failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2)	its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification,	The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(E-ISAC) according to Requirement R2, Attachment 1, Section 4.		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but	The Responsible Entity has used delegated authority for actions where allowed by the CIP

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specific actions delegated, but 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. (R4)	specific actions delegated, but 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. (R4)	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. (R4)	Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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.	

Version	Date	Action	Change Tracking
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 devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees.	Revised to address FERC Order 822 directive regarding definition of LERC.

Attachment 1

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

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

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

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

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security ~~control~~ objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term ~~"direct"~~'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule~~."~~."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii~~) which reads:~~): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The

focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

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

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

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

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and~~,~~

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g.~~,~~ communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Attachment 2

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

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

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

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

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

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

1. Documentation~~, such as representative diagrams or lists of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; implementing unidirectional gateways)~~ showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices~~; and~~ . Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of

implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible ~~Entity is not~~Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this ~~can~~may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a

combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The ~~requirement does~~standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). ~~The~~The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities ~~are~~ to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such

communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, ~~any~~it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), ~~does not require evaluation~~to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

~~In order for Responsible Entities to~~To determine whether electronic access controls need to be implemented, the Responsible Entity ~~needs~~has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that ~~use~~uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach ~~to making this evaluation.~~. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the

Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity ~~documents~~to document and ~~implements~~implement its chosen electronic access control(s). The control(s) ~~must~~are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. ~~The~~However the Responsible Entity ~~must be~~chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for ~~the~~ "necessary" inbound and outbound electronic access controls ~~can~~may be documented within the Responsible Entity's cyber security plan(s~~)~~), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

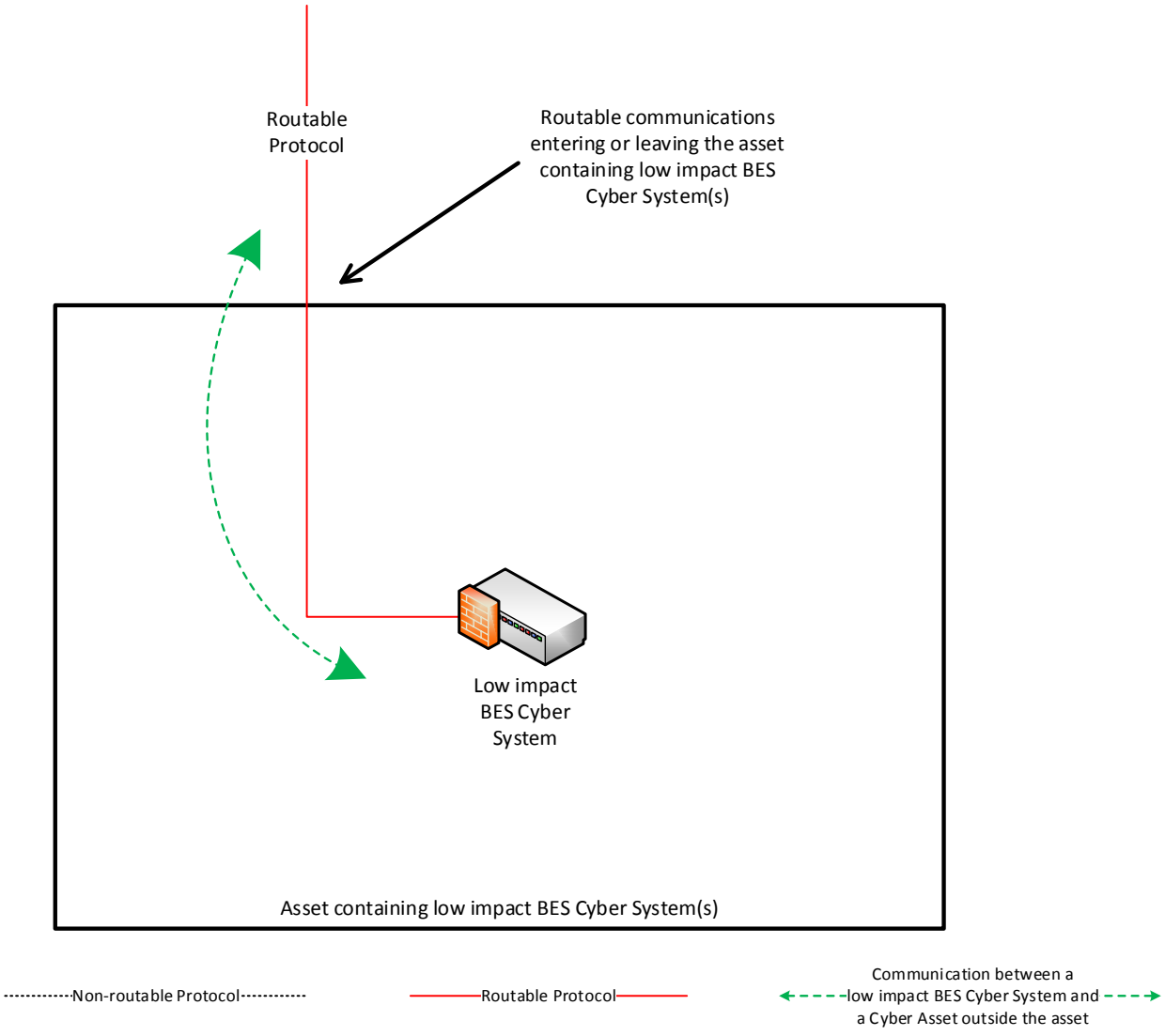
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset ~~must be met~~.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

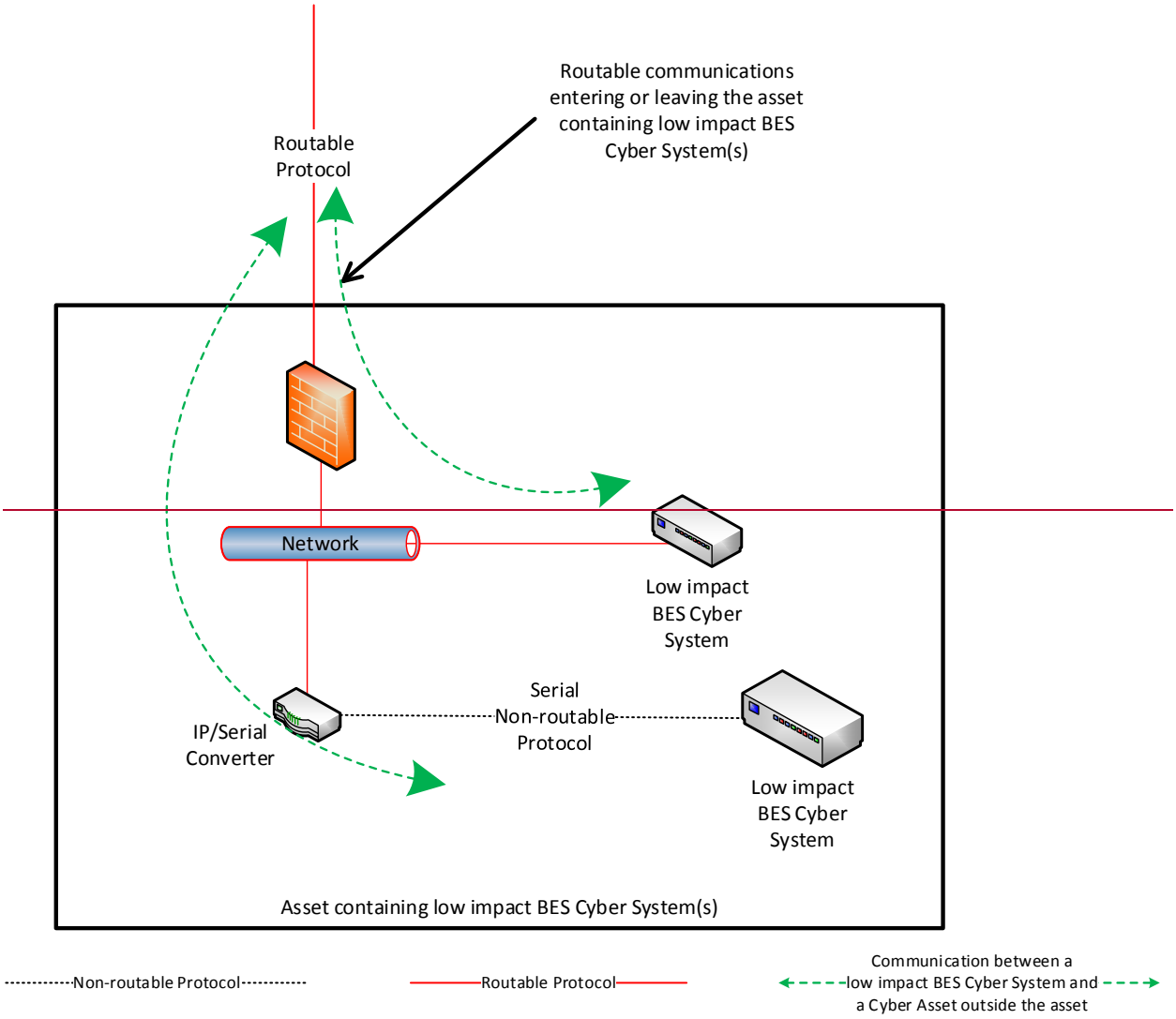
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound ~~routable protocol~~electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions~~, at a minimum~~ using access control lists, the ~~permissions need to~~Responsible Entity could restrict communication(s) using source and destination addresses~~,~~ or ~~a range~~ranges of addresses ~~when necessary.~~. Responsible Entities ~~may further~~could also restrict ~~electronic access~~communication(s) using ports ~~and~~or services based on the capability of the electronic access control, the low impact BES Cyber System~~,~~(s), or the application~~, etc.~~(s).

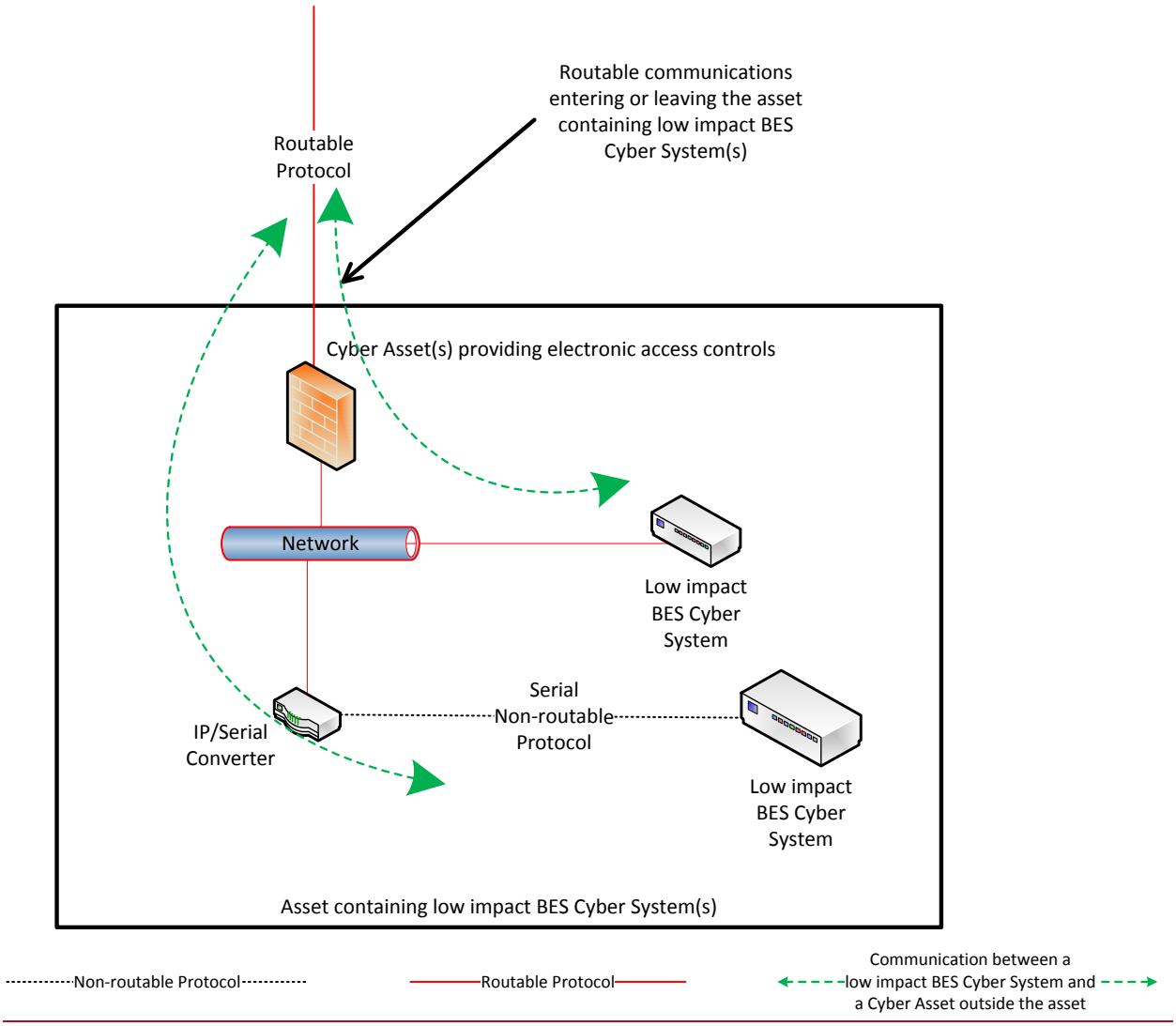


Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions~~, at a minimum~~ using access control lists, the ~~permissions need to~~Responsible Entity could restrict communication(s) using source and destination addresses~~,~~ or ~~a range~~ranges of addresses~~ when necessary.~~. Responsible Entities ~~may further~~could also restrict ~~electronic access~~communication(s) using ports ~~and~~or services based on the capability of the electronic access control, the low impact BES Cyber System~~,~~(s), or the application~~, etc.~~(s).

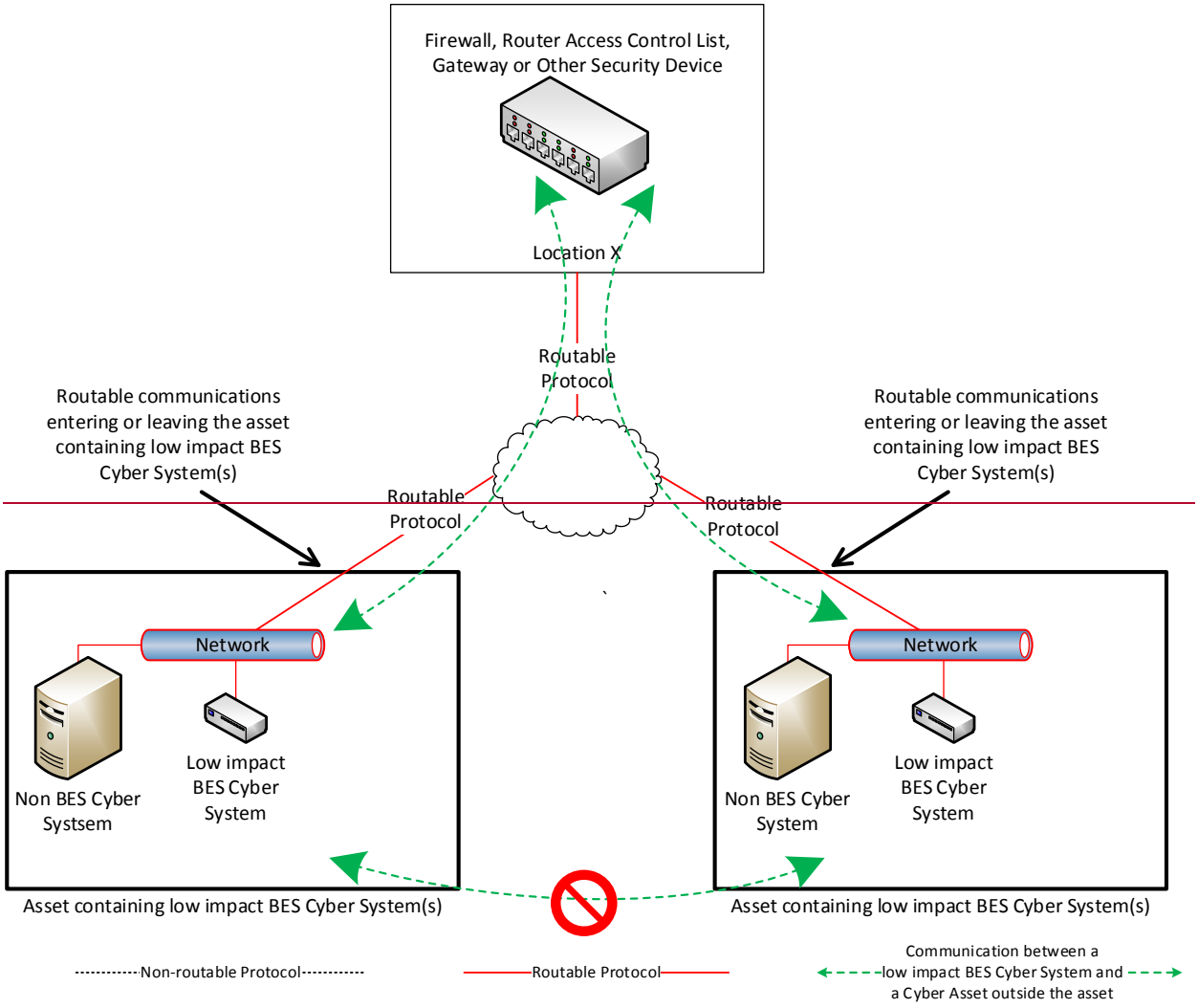


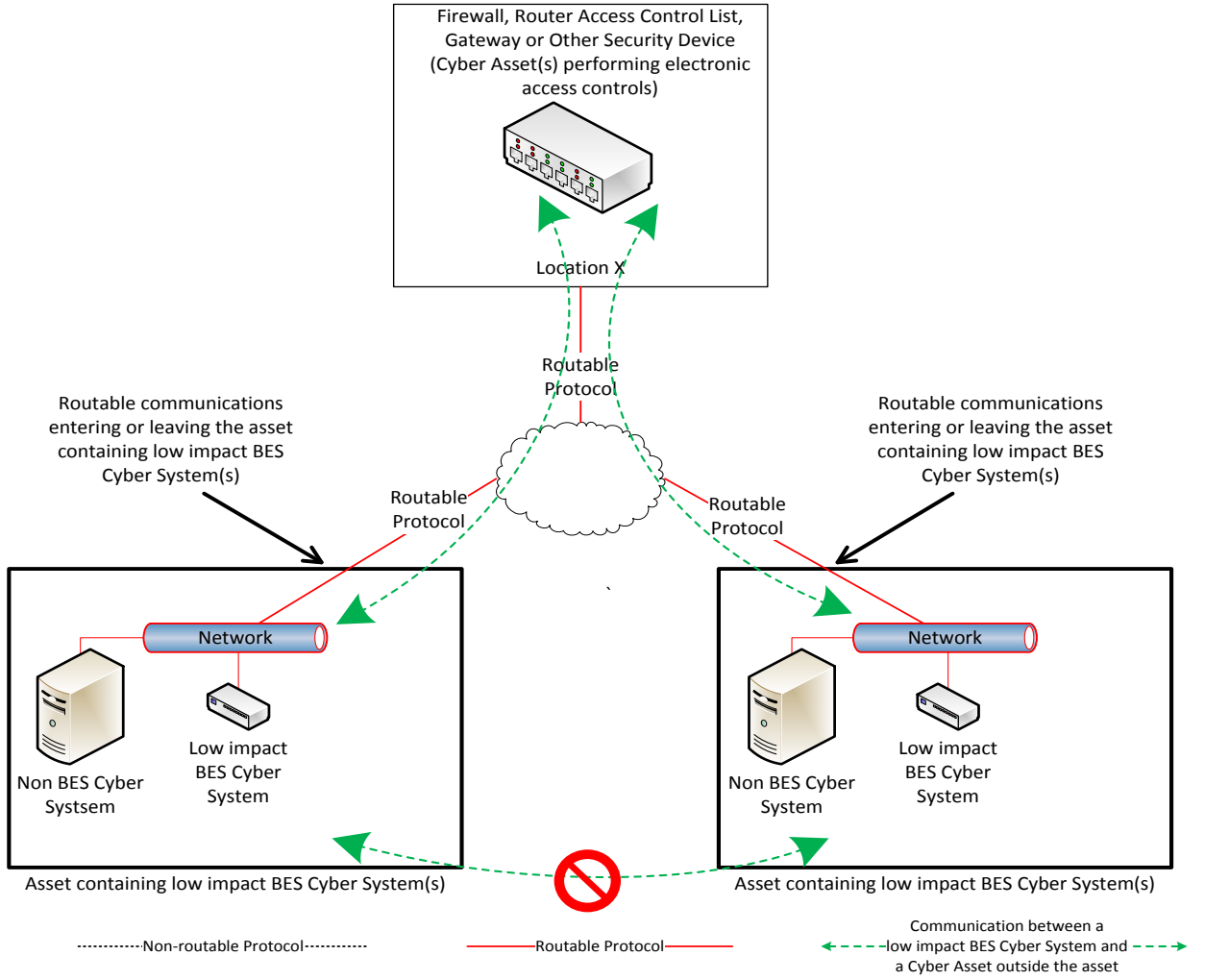


Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions~~, at a minimum~~ using access control lists, the ~~permissions need to~~Responsible Entity could restrict communication(s) using source and destination addresses~~,~~ or ~~a range~~ranges of addresses~~ when necessary.~~. Responsible Entities ~~can further~~could also restrict ~~electronic access~~communication(s) using ports ~~and~~or services based on the capability of the electronic access control, the low impact BES Cyber System~~,~~(s), or the application~~, etc.~~(s).

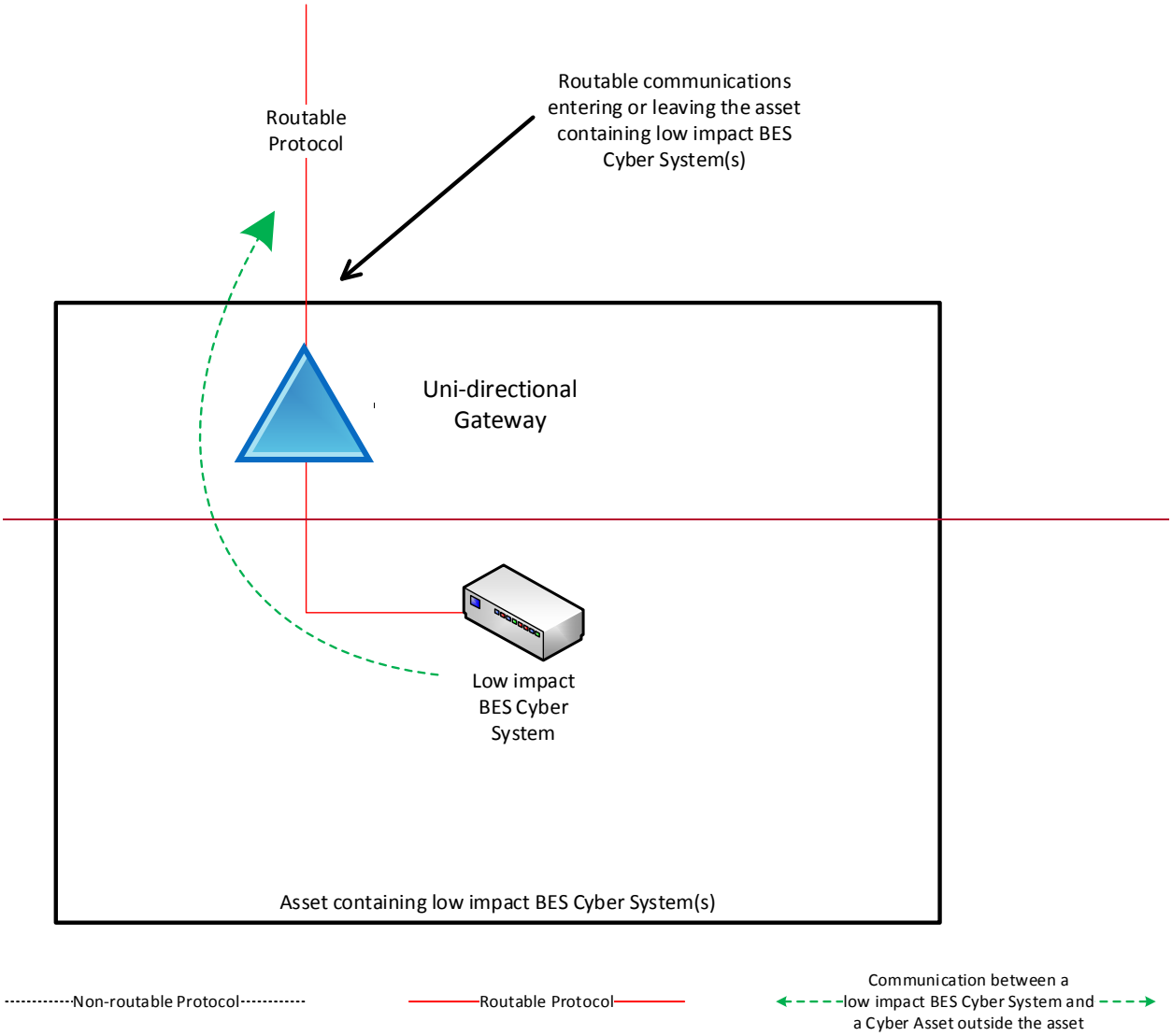

Firewall, Router Access Control List, Gateway or Other Security Device
Location X
Routable Protocol
Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
Routable Protocol
Routable Protocol
Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
Network
Non BES Cyber Systsem
Low impact BES Cyber System
Network
Non BES Cyber System
Low impact BES Cyber System
Asset containing low impact BES Cyber System(s)
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

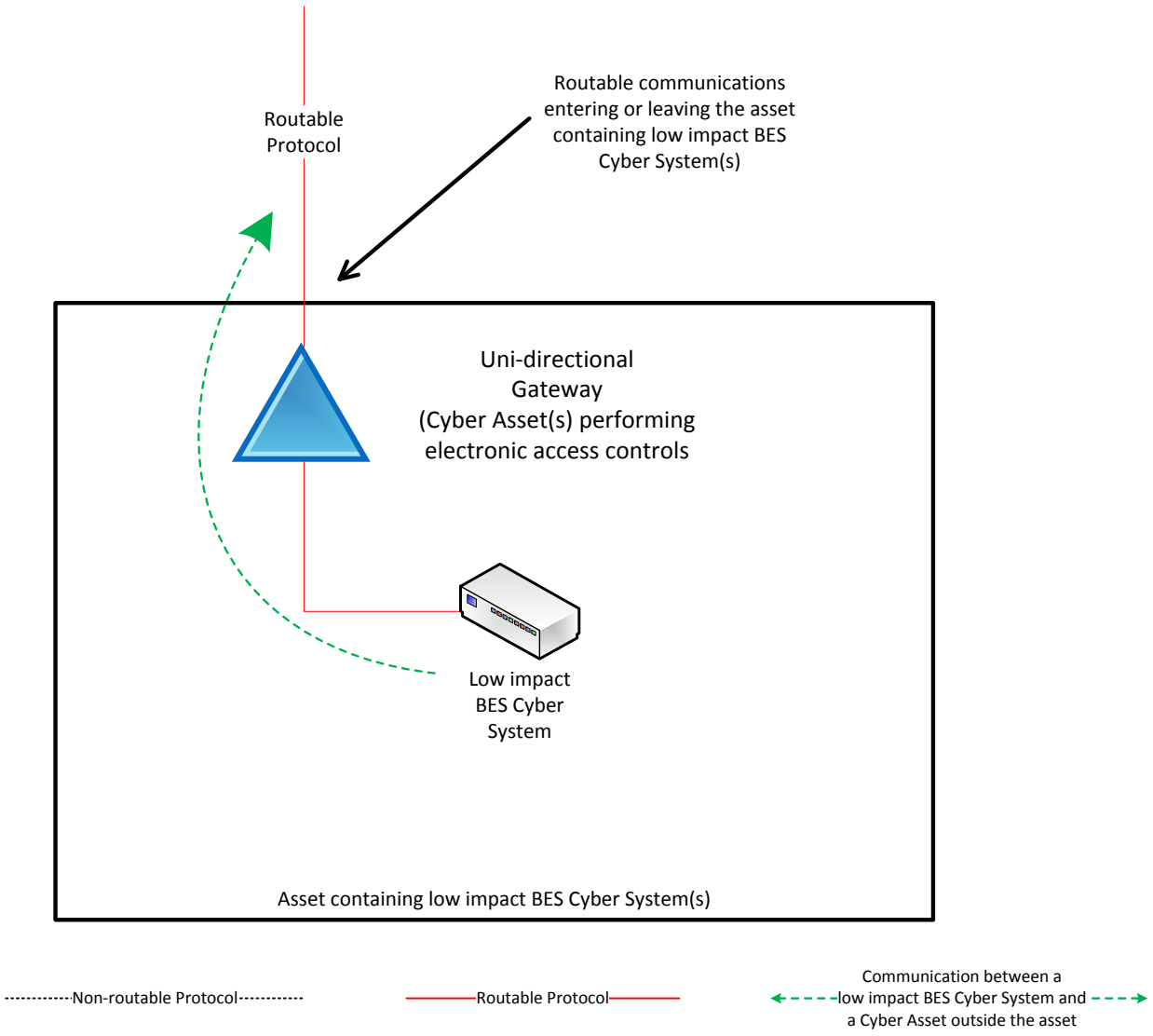


Reference Model 3

Reference Model 4 – Uni-directional Gateway

The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.

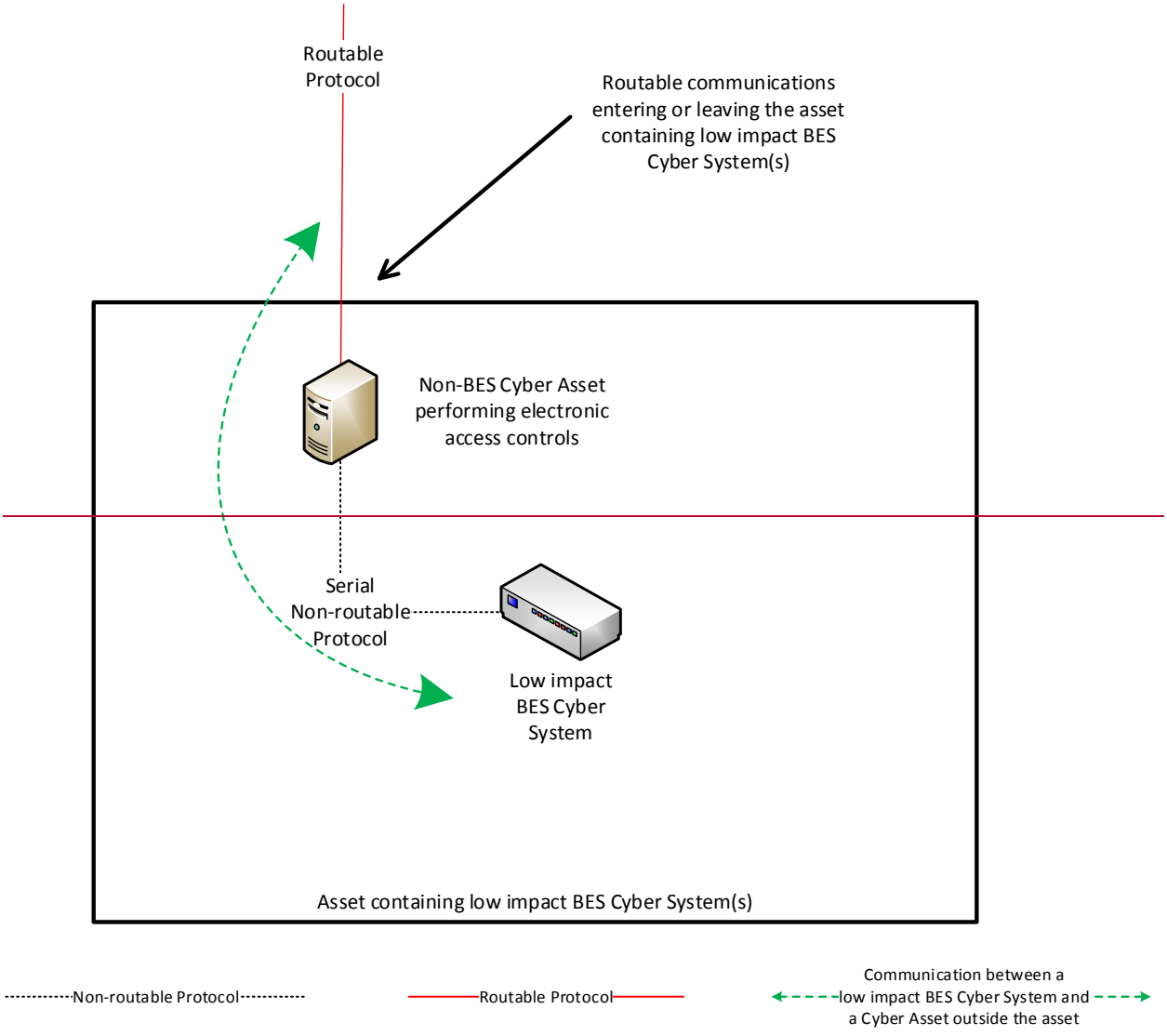


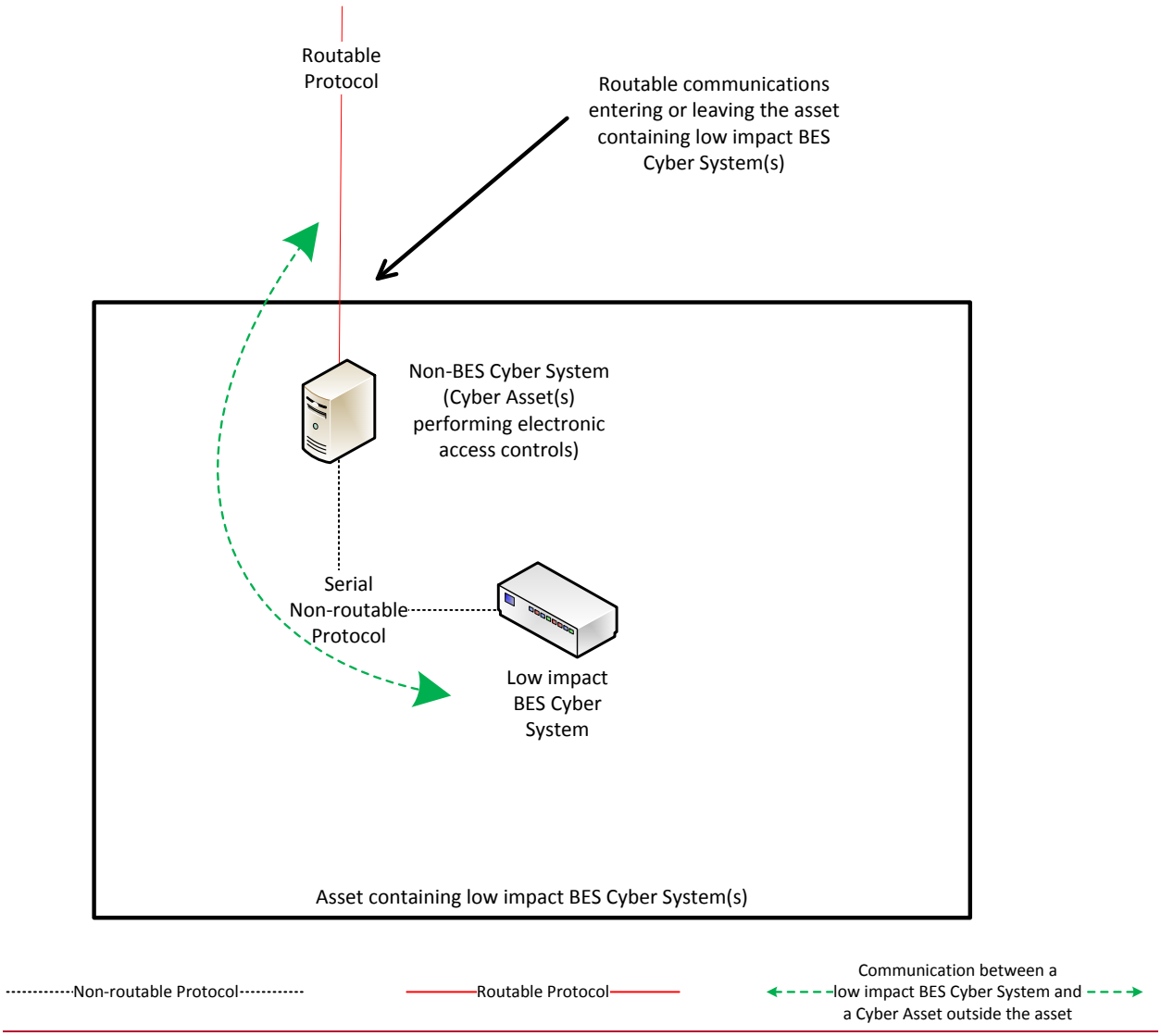


Reference Model 4

Reference Model 5 – User Authentication

This reference model demonstrates that Responsible Entities have flexibility in choosing ~~their~~ electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication ~~must be~~is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications ~~may~~would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.

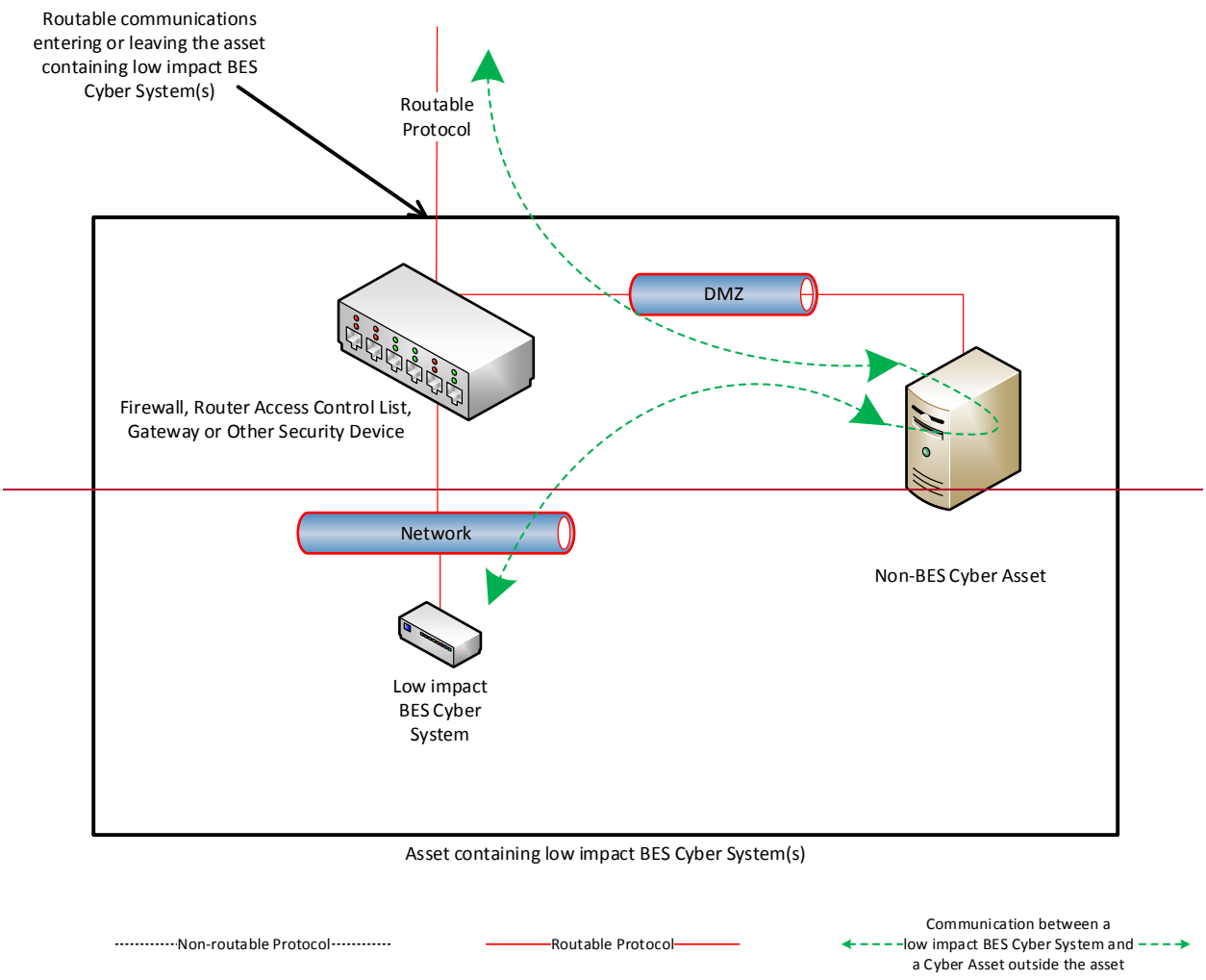


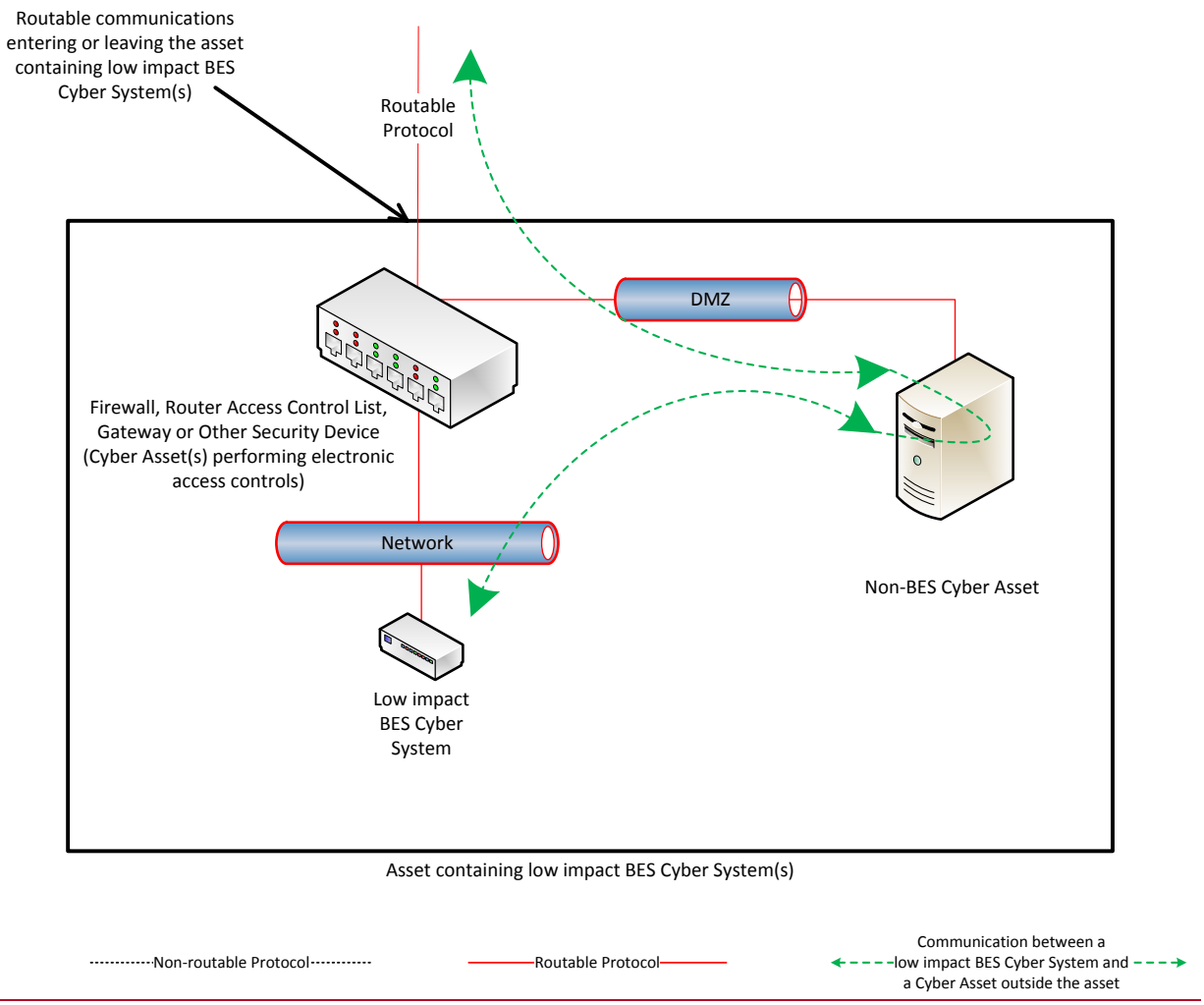


Reference Model 5

Reference Model 6 – Indirect Access

In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity ~~needs to~~ implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, ~~this~~the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.

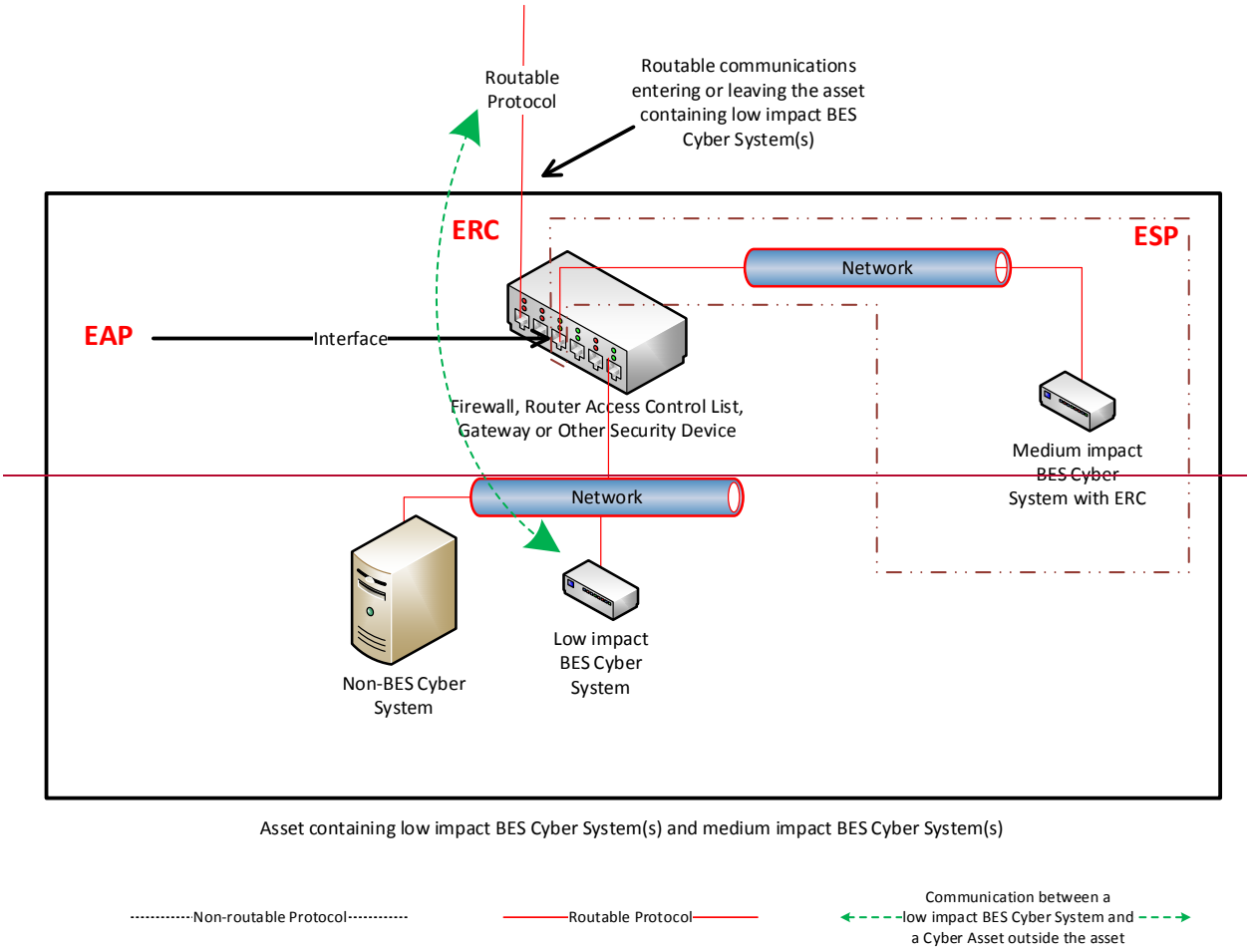

Routable communications entering or leaving the asset containing low impact BES Cyber System(s)
Routable Protocol
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset
Low impact BES Cyber System
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset

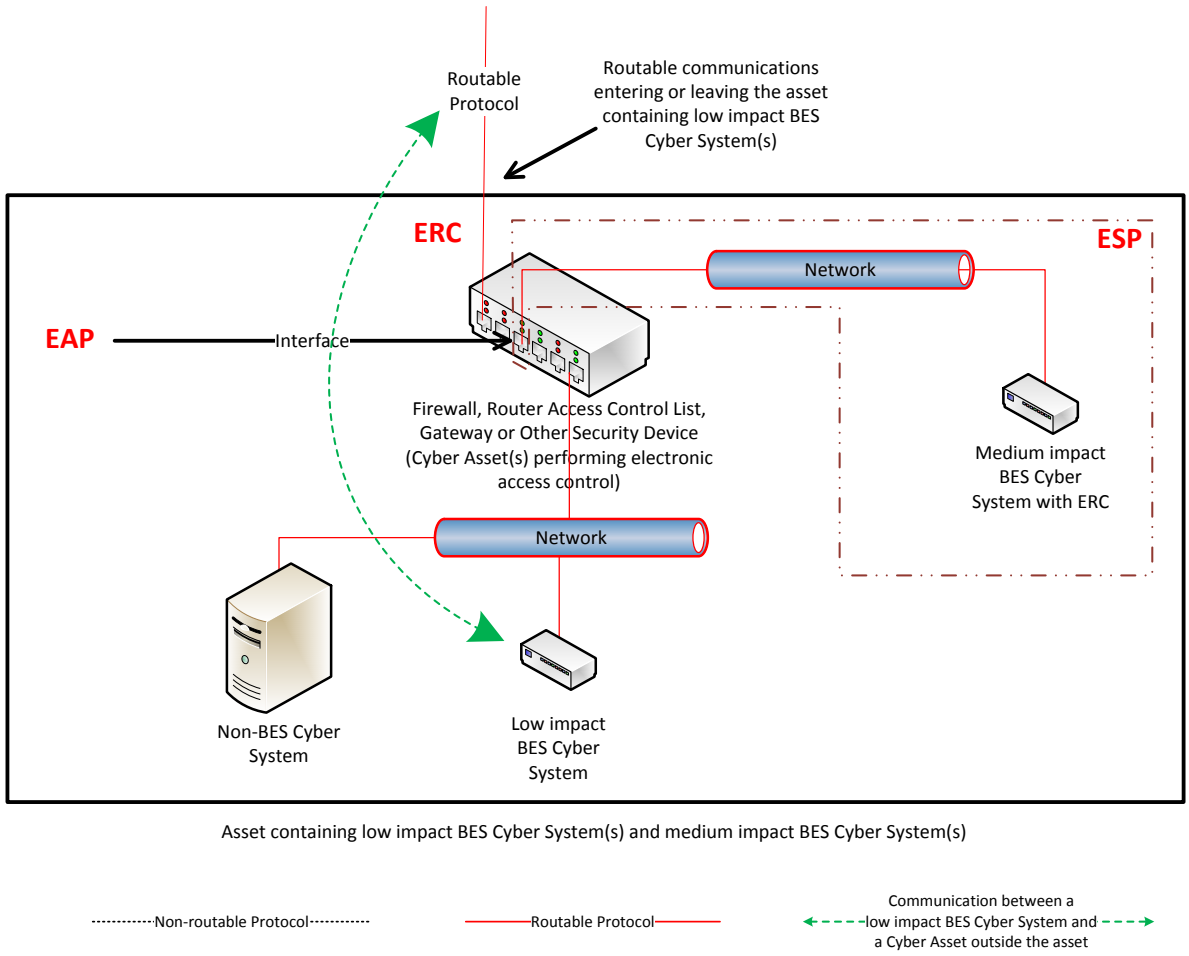


Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

~~There~~In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and ~~ERC present in this reference model~~External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls~~.~~ for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.





Reference Model 7

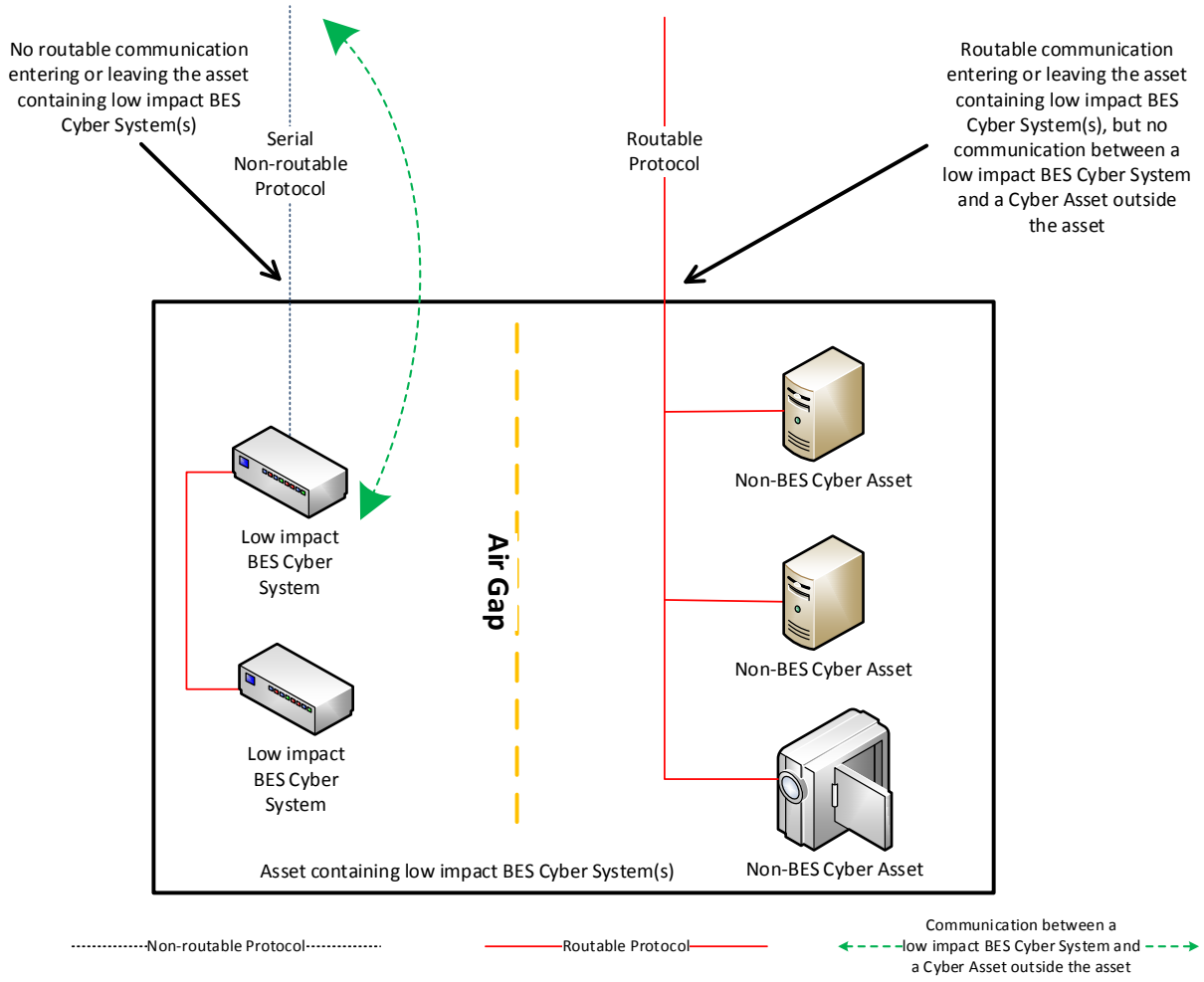
Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria ~~for~~from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;

2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls~~; and~~.

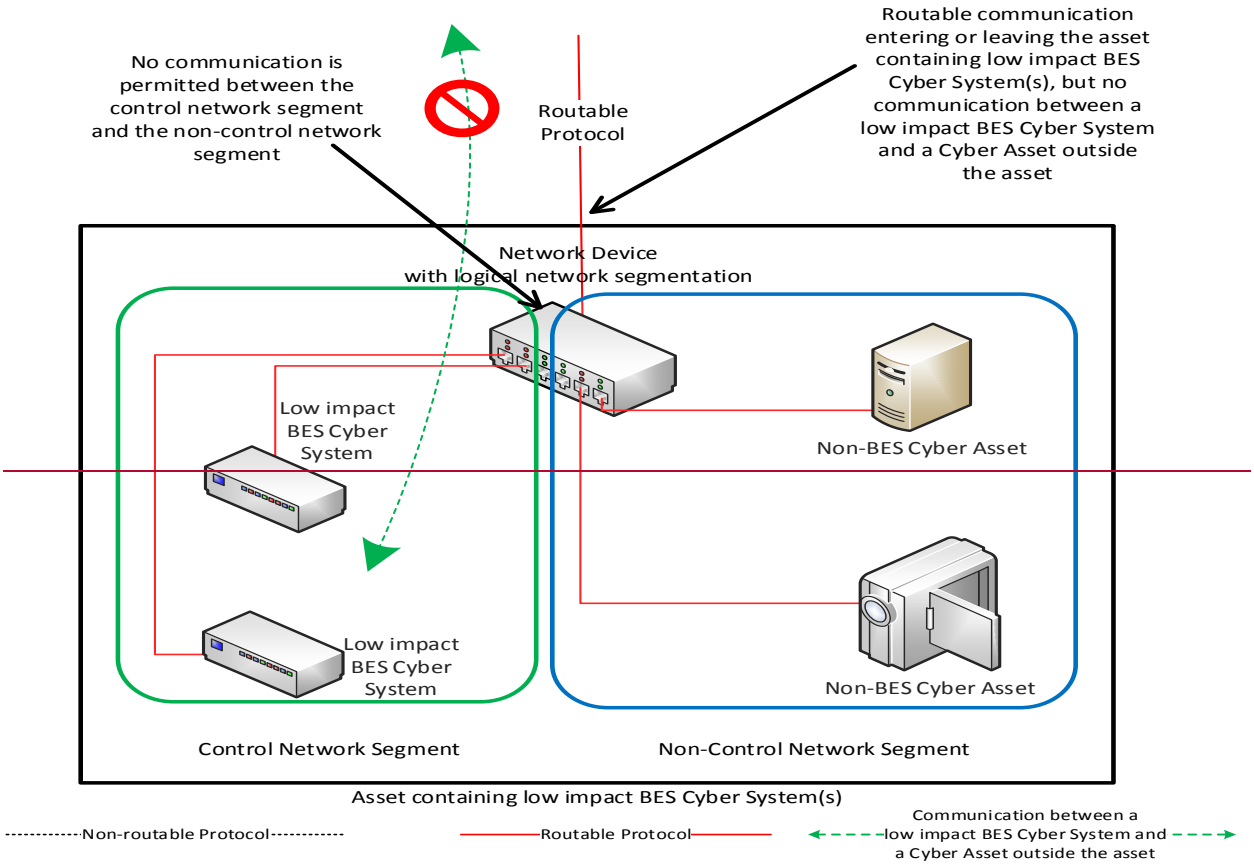
~~3)~~ The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).

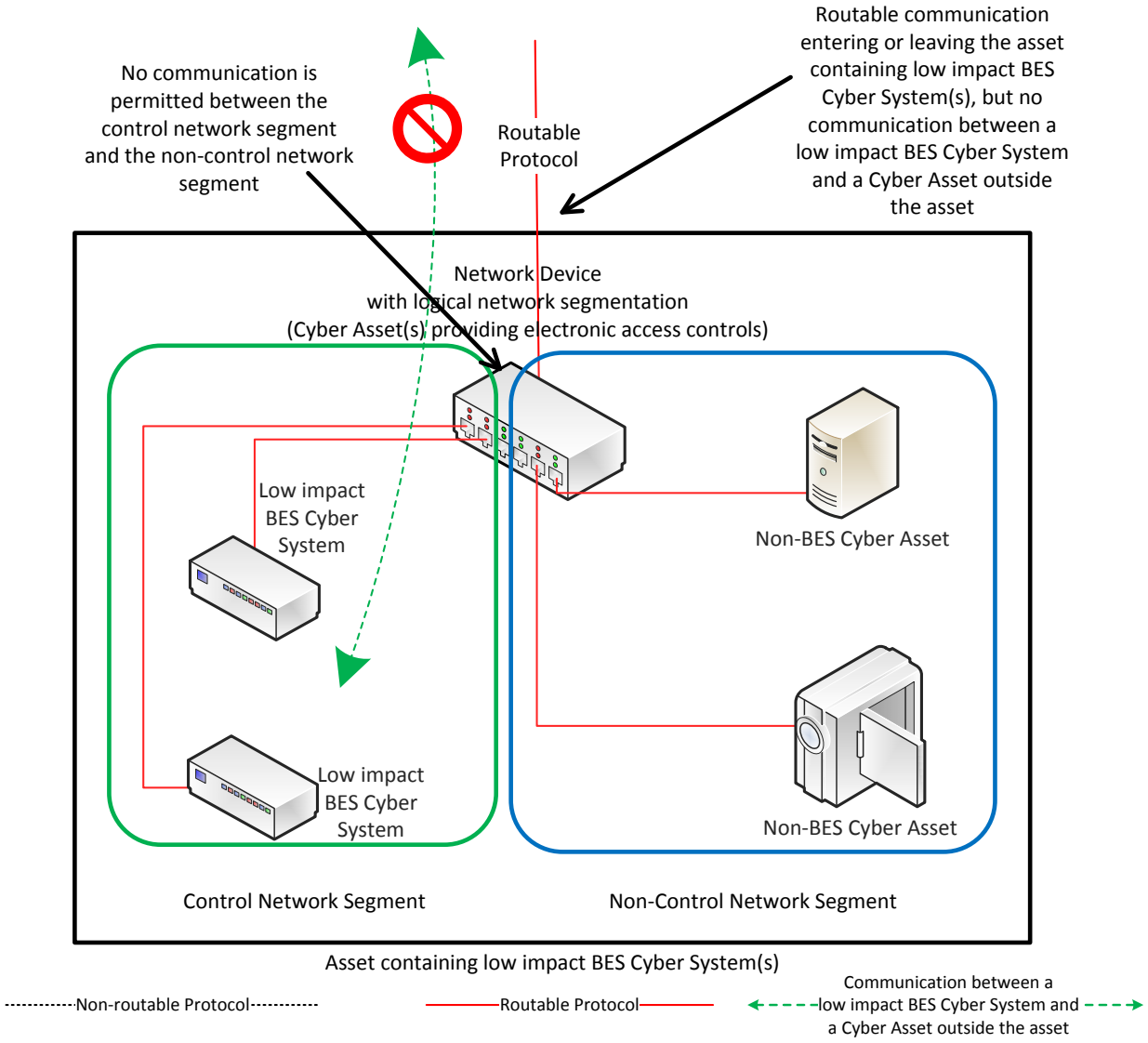


Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

In this reference model, the criteria ~~for~~from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.

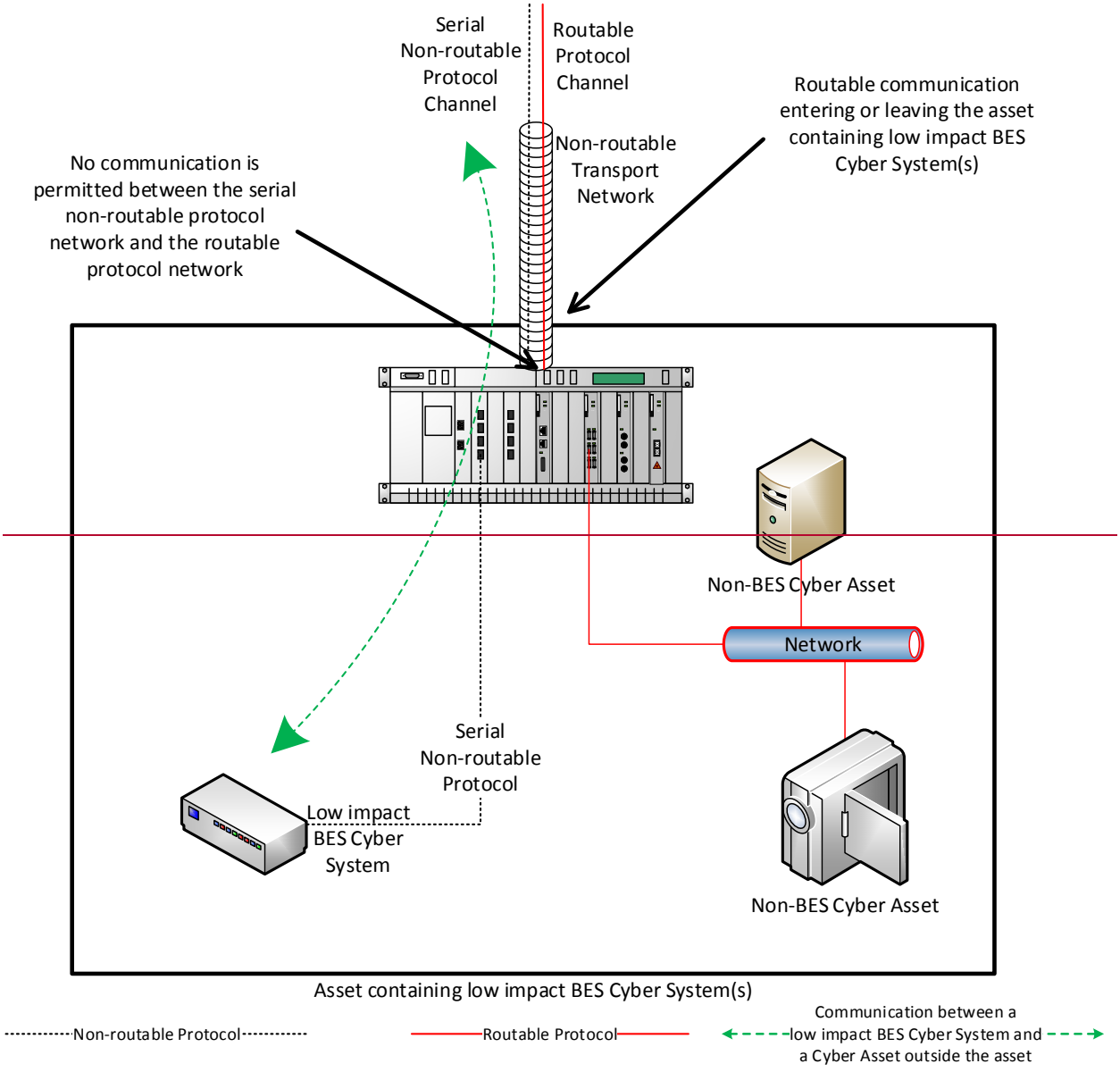


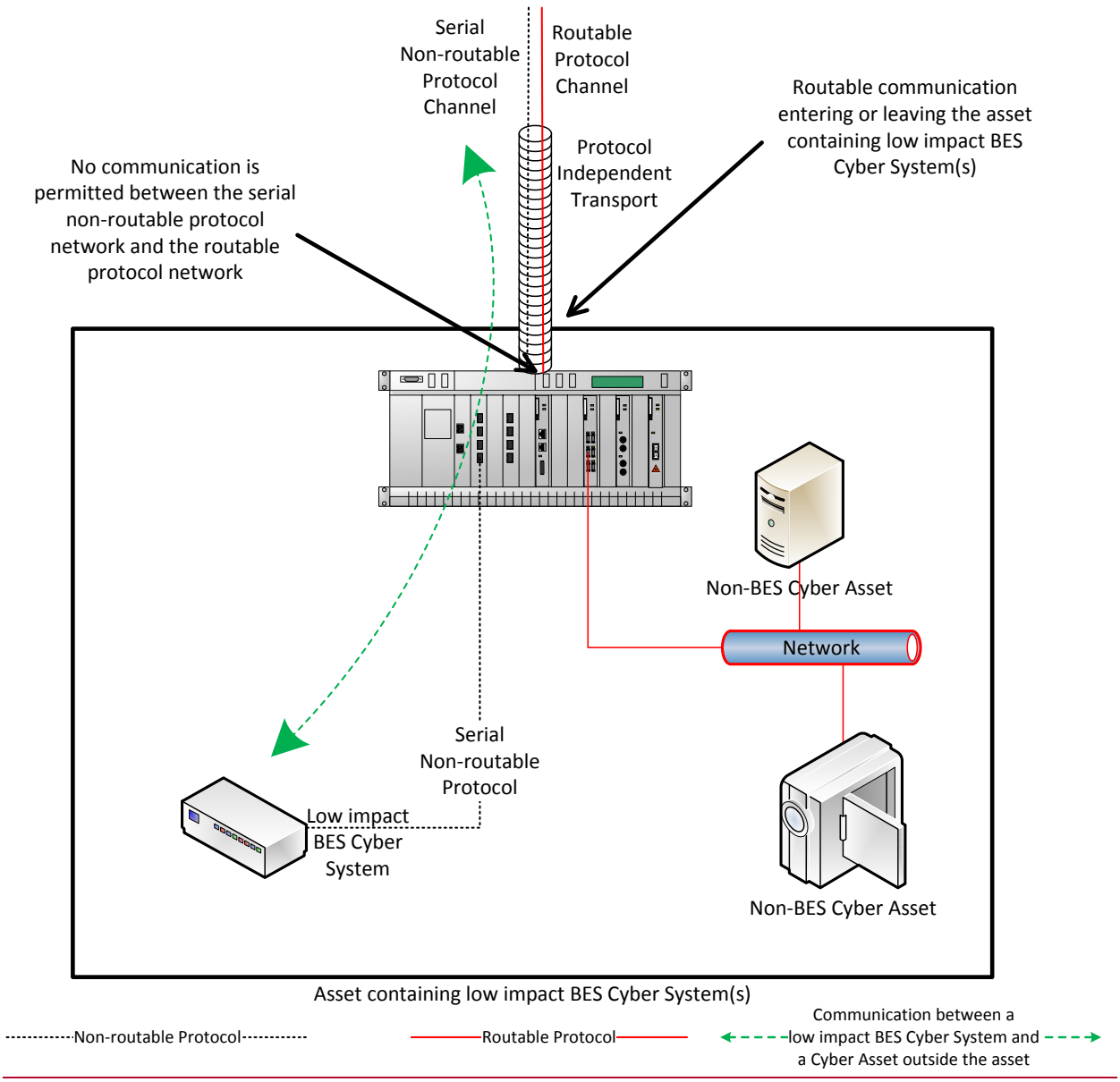


Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable ~~technology,~~communication such as a Time-Division Multiplexing (TDM) ~~or~~network, a Synchronous Optical Network (SONET~~) network. In this reference model, the criteria requiring electronic access controls are not met~~), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol. ~~In similar configurations, the Responsible Entity should closely evaluate the transport entering or leaving the asset containing low impact BES Cyber System(s). If the communication entering or leaving the asset containing low impact BES Cyber System(s) was routable (such as serial encapsulated in TCP/IP or UDP/IP as depicted Reference Model 2 or Reference Model 5), then the criteria requiring electronic access controls would be met.~~


Serial Non-routable Protocol Channel
Routable Protocol Channel
Routable communication entering or leaving the asset containing low impact BES Cyber System(s)
Non-routable Transport Network
No communication is permitted between the serial non-routable protocol network and the routable protocol network
Non-BES Cyber Asset
Network
Serial Non-routable Protocol
Low impact BES Cyber System
Non-BES Cyber Asset
Asset containing low impact BES Cyber System(s)
Non-routable Protocol
Routable Protocol
Communication between a low impact BES Cyber System and a Cyber Asset outside the asset



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-003-7 - Cyber Security – Security Management Controls

Requested Approvals

- Reliability Standard CIP-003-7 - Cyber Security – Security Management Controls

Requested Retirements

- Reliability Standard CIP-003-6 - Cyber Security – Security Management Controls
- Definition Low Impact BES Cyber System Electronic Access Point (LEAP)
- Definition of Low Impact External Routable Connectivity (LERC)

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards*, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions. In addition to approving the seven CIP Reliability Standards, the Commission, among other things, directed NERC to modify the definition of LERC. The Commission stated:

> 73. Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity

definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

As an alternative to modifying the definition consistent with the Commission's directive, the standard drafting team retired the term "LERC" and incorporated the LERC concepts within the requirement language.

Given the proposed retirement of the LERC definition and the proposed modifications in Reliability Standard CIP-003-7, there is no longer a need for the NERC Glossary term Low Impact BES Cyber System Electronic Access Point (LEAP). Consequently, NERC is proposing to retire the term LEAP.

General Considerations

The effective dates or phased-in compliance dates within the CIP-003-6 Implementation Plan, remain in effect except that the compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7.

The Responsible Entity shall not be required to include in its cyber security plan(s) elements related to Sections 2 and 3 of Attachment 1 until the effective date of CIP-003-7. Upon the effective date of CIP-003-7, the Responsible Entity's cyber security plan(s) must include the elements required by Sections 2 and 3 of Attachment 1 and the Responsible Entity must implement the controls included in its plan to meet the objectives of Sections 2 and 3.

Effective Date

The effective date for the proposed Reliability Standard is provided below:

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7 shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-7 shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Planned or Unplanned Changes

Planned or Unplanned Changes Resulting in a Higher Categorization – This Implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-5 titled Planned or Unplanned Changes Resulting in a Higher Categorization.[1]

Unplanned Changes Resulting in Low Impact Categorization – This Implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-6 titled Unplanned Changes Resulting in Low Impact Categorization. That section provides:

> For unplanned changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

Retirement Date

Reliability Standard CIP-003-6

Reliability Standard CIP-003-6 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-7 in the particular jurisdiction in which the revised standard is becoming effective.

Current NERC Glossary of Terms of LERC and LEAP

The current definition of LERC and the term LEAP shall be retired from the NERC Glossary of Terms immediately prior to the effective date of CIP-003-7 in the particular jurisdiction in which the definition is becoming effective.

[1] Due to the length of that section, it is not reproduced herein.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-003-7 - Cyber Security – Security Management Controls ~~and Low Impact External Routable Communication (LERC)~~

Requested Approvals

- Reliability Standard CIP-003-7 - Cyber Security – Security Management Controls

Requested Retirements

- Reliability Standard CIP-003-6 - Cyber Security – Security Management Controls
- Definition Low Impact BES Cyber System Electronic Access Point (LEAP)
- Definition of Low Impact External Routable Connectivity (LERC)

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards*, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions. In addition to approving the seven CIP Reliability Standards, the Commission, among other things, directed NERC to modify the definition of LERC. The Commission stated:

> 73. Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to

address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

As an alternative to modifying the definition consistent with the Commission's directive, the standard drafting team retired the term "LERC" and ~~incorpored~~incorporated the LERC concepts within the requirement language.

Given the proposed retirement of the LERC definition and the proposed modifications in Reliability Standard CIP-003-7, there is no longer a need for the NERC Glossary term Low Impact BES Cyber System Electronic Access Point (LEAP). Consequently, NERC is proposing to retire the term LEAP.

General Considerations

The effective dates or phased-in compliance dates within the CIP-003-6 Implementation Plan, remain in effect except that the compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7.

The Responsible Entity shall not be required to include in its cyber security plan(s) elements related to Sections 2 and 3 of Attachment 1 until the effective date of CIP-003-7. Upon the effective date of CIP-003-7, the Responsible Entity's cyber security plan(s) must include the elements required by Sections 2 and 3 of Attachment 1 and the Responsible Entity must implement the controls included in its plan to meet the objectives of Sections 2 and 3.

Effective Date

The effective date for the proposed Reliability Standard is provided below:

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7 shall become effective on the ~~later of September 1, 2018 or the~~ first day of the first calendar quarter that is ~~twelve (12~~eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-7 shall become effective on the first day of the first calendar quarter that is ~~twelve (12~~eighteen (18) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Planned or Unplanned Changes

Planned or Unplanned Changes Resulting in a Higher Categorization – This Implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-5 titled Planned or Unplanned Changes Resulting in a Higher Categorization.[1]

Unplanned Changes Resulting in Low Impact Categorization – This Implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-6 titled Unplanned Changes Resulting in Low Impact Categorization. That section provides:

> For unplanned changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

Retirement Date

Reliability Standard CIP-003-6

Reliability Standard CIP-003-6 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-7 in the particular jurisdiction in which the revised standard is becoming effective.

Current NERC Glossary of Terms of LERC and LEAP

The current definition of LERC and the term LEAP shall be retired from the NERC Glossary of Terms immediately prior to the effective date of CIP-003-7 in the particular jurisdiction in which the definition is becoming effective.

[1] Due to the length of that section, it is not reproduced herein.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards
CIP-003-7

Final Ballot Open through December 19, 2016

Now Available

Final ballots for **CIP-003-7 - Cyber Security – Security Management Controls** and the **CIP-003-7 Implementation Plan** are open through **8 p.m. Eastern, Monday, December 19, 2016.**

Balloting

In the final ballot, votes are counted by exception. Votes from the previous ballot are automatically carried over in the final ballot. Only members of the applicable ballot pools can cast a vote. Ballot pool members who previously voted have the option to change their vote in the final ballot. Ballot pool members who did not cast a vote during the previous ballot can vote in the final ballot.

Members of the ballot pools associated with this project can log in and submit their votes here. If you experience any difficulties using the Standards Balloting & Commenting System (SBS), contact Wendy Muller.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The voting results will be posted and announced after the ballot closes. If approved, the standard and implementation plan will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Standards Development Process

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Al McMeekin (via email) or at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards CIP-003-7 FN 3 ST
Voting Start Date: 12/9/2016 11:52:05 AM
Voting End Date: 12/19/2016 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 3
Total # Votes: 281
Total Ballot Pool: 339
Quorum: 82.89
Weighted Segment Value: 87.95

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	54	0.818	12	0.182	0	5	15
Segment: 2	7	0.1	1	0.1	0	0	0	2	4
Segment: 3	75	1	55	0.887	7	0.113	0	2	11
Segment: 4	26	1	17	0.895	2	0.105	0	2	5
Segment: 5	80	1	52	0.839	10	0.161	0	3	15
Segment: 6	48	1	35	0.814	8	0.186	0	1	4
Segment: 7	3	0	0	0	0	0	0	1	2
Segment: 8	3	0.2	2	0.2	0	0	0	0	1
Segment: 9	2	0.2	2	0.2	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.7	7	0.7	0	0	0	1	1
Totals:	339	6.2	225	5.453	39	0.747	0	17	58

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	Andrew Pusztai		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Affirmative	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Devin Elverdi		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		Abstain	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Negative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass	Matt Stryker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Abstain	N/A
1	JEA	Ted Hobson	Joe McClung	None	N/A
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		None	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Negative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Negative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Affirmative	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Abstain	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Abstain	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Negative	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Negative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry Bllke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		None	N/A
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		Abstain	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		None	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Negative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Affirmative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Affirmative	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Affirmative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		None	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Abstain	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		Affirmative	N/A
4	Austin Energy	Tina Garvey		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Affirmative	N/A
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		None	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Abstain	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Negative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Affirmative	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Negative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		Affirmative	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Affirmative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		None	N/A
5	Lakeland Electric	Jim Howard	Chris Gowder	None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Abstain	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Erick Barrios		Negative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		Affirmative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		None	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Abstain	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Abstain	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Negative	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		Affirmative	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Affirmative	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Snohomish County PUD No. 1	Franklin Lu		Negative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	N/A
6	Westar Energy	Megan Wagner		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		Abstain	N/A
7	Luminant Mining Company LLC	Stewart Rake		None	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		None	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Abstain	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 339 of 339 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards CIP-003-7 Implementation Plan FN 3 OT
Voting Start Date: 12/9/2016 11:52:41 AM
Voting End Date: 12/19/2016 8:00:00 PM
Ballot Type: OT
Ballot Activity: FN
Ballot Series: 3
Total # Votes: 281
Total Ballot Pool: 338
Quorum: 83.14
Weighted Segment Value: 83.03

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	56	0.824	12	0.176	0	3	14
Segment: 2	7	0.1	1	0.1	0	0	0	2	4
Segment: 3	75	1	49	0.79	13	0.21	0	2	11
Segment: 4	26	1	15	0.75	5	0.25	0	1	5
Segment: 5	80	1	48	0.774	14	0.226	0	3	15
Segment: 6	48	1	34	0.81	8	0.19	0	2	4
Segment: 7	3	0	0	0	0	0	0	1	2
Segment: 8	3	0.2	2	0.2	0	0	0	0	1
Segment: 9	2	0.2	2	0.2	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.7	7	0.7	0	0	0	1	1
Totals:	338	6.2	214	5.148	52	1.052	0	15	57

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	Andrew Pusztai		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	Negative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Affirmative	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Devin Elverdi		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		Abstain	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Negative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass	Matt Stryker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec Production	Aviance Freeman		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	None	N/A
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		None	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Negative	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Abstain	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Negative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	N/A
1	Westar Energy	Kevin Giles		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry Bllke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		None	N/A
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		Abstain	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		Negative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Negative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		None	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Negative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Affirmative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Negative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Negative	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Affirmative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		None	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Negative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Negative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Abstain	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		Negative	N/A
4	Austin Energy	Tina Garvey		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Affirmative	N/A
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Negative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Negative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Michael Ward		Affirmative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	N/A
5	AEP	Thomas Foltz		Negative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Affirmative	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Negative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		Affirmative	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Affirmative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		None	N/A
5	Lakeland Electric	Jim Howard	Chris Gowder	None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Abstain	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Abstain	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Erick Barrios		Negative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Negative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		Affirmative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		None	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Abstain	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		Affirmative	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Negative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Negative	N/A
5	Xcel Energy, Inc.	David Lemmons		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Affirmative	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Snohomish County PUD No. 1	Franklin Lu		Negative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	N/A
6	Westar Energy	Megan Wagner		Negative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		Abstain	N/A
7	Luminant Mining Company LLC	Stewart Rake		None	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		None	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 338 of 338 entries

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.

Description of Current Draft

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions to be incorporated into the Glossary of Terms Used in NERC Reliability Standards. In addition to approving the seven CIP Reliability Standards, the Commission, directed NERC to, among other things,: (1) "…develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems…", and (2) modify the definition of LERC.

In response to these directives, NERC first modified Reliability Standard CIP-003-6 to address the LERC directive, which has a regulatory deadline of March 31, 2017 for filing with the Commission. The revisions associated with the LERC directive were developed and posted for comment and ballot in July 2016 in draft Reliability Standard CIP-003-7. The revisions were not approved by stakeholders and based on the feedback received, the drafting team revised its approach and posted the revisions for an additional comment period and ballot. CIP-003-7 passed the additional ballot that ended on December 5, 2016.

For the transient device directive, NERC initially posted draft revisions for an informal comment period from November 1-18, 2016. This draft of Reliability Standard CIP-003-7(i) incorporates the proposed TCA language, as modified based on stakeholder comment, with the recently passed LERC revisions. The intent of this approach is to allow entities time to efficiently plan and implement the required modifications for low impact BES Cyber Systems. The Standard Drafting Team (SDT) approach to address the transient device directive is summarized below.

The SDT revised Attachment 1 of CIP-003-7 to include requirements that mitigate the risk to the BES of malware propagation from transient devices to low impact BES Cyber Systems. Attachment 1 contains and outlines the required sections of a Responsible Entity's cyber security plan(s) for its low impact BES Cyber Systems per Requirement R2. Previously, cyber security plan(s) were required to address four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. In keeping with the stakeholder approved approach to incorporate into one standard all the requirements applicable to assets containing low impact BES Cyber Systems, the SDT expanded CIP-003-7 Attachment 1 to include a fifth area: "Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation." Requiring the Responsible Entity to develop and implement these plans will provide higher assurance against the propagation of malware from transient devices.

In addition, the SDT determined it was necessary to revise the definitions of a Transient Cyber Asset (TCA) and Removable Media to ensure applicability of security controls and provide additional clarity. As well, the revised definitions accommodate use of the terms for all impact

levels: high, medium, and low. This is important for those entities that may opt to deploy one program to manage TCAs and Removable Media across multiple impact level assets.

The proposed revised definition of a Transient Cyber Asset (TCA) is:

A Cyber Asset that is:

1. *capable of transmitting or transferring executable code,*
2. *not included in a BES Cyber System,*
3. *not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and*
4. *directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:*
    - *BES Cyber Asset,*
    - *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
    - *PCA associated with high or medium impact BES Cyber Systems.*

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

The proposed revised definition of Removable Media is:

Storage media that:

1. *are not Cyber Assets,*
2. *are capable of transferring executable code,*
3. *can be used to store, copy, move, or access data, and*
4. *are directly connected for 30 consecutive calendar days or less to a:*
    - *BES Cyber Asset,*
    - *network within an Electronic Service Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
    - *Protected Cyber Asset associated with high or medium impact BES Cyber Systems.*

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

As proposed, Section 5 of Attachment 1 of CIP-003-7(i) mandates that entities have malware protection on TCAs (both entity and vendor-managed) and for Removable Media. The SDT proposes that it is necessary to distinguish between the specific protections for: (i) TCAs managed by the Responsible Entity, (ii) TCAs managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media.

For TCAs managed by the Responsible Entity, Section 5 requires the Responsible Entity to use one or a combination of the following to mitigate the introduction of malicious code: antivirus software, application whitelisting, or some other method. The SDT recognizes that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices (i.e., manage in an ongoing manner) while others have a checklist for transient devices prior to connecting them to a BES Cyber System (i.e., manage in an on-demand manner). The SDT acknowledges that both methods are effective and Section 5 permits either form of management. Because of the higher frequency in which these entity-managed devices are used, the controls required for these devices are more specific.

For Transient Cyber Assets managed by a party other than the Responsible Entity, Section 5 requires the Responsible Entity to review and verify the malware mitigation mechanism(s) used by the third party prior to connecting the Transient Cyber Asset (per Transient Cyber Asset capability).

For Removable Media, Section 5 requires entities to employ methods to detect malicious code and mitigate the threat of detected malicious code prior to connecting to a low impact BES Cyber System.

In summary, the SDT made the following changes to address the directive:

1. Revised the definitions of Transient Cyber Asset (TCA) and Removable Media.
2. Revised Requirement R1, by adding Parts 1.2.5 and 1.2.6 to include the complementary policies for the Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation in Requirement R2 (Attachment 1 of CIP-003-7(i)).
3. Revised the requirement language (Requirement R2) in Attachment 1 of CIP-003-7 by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation.
4. Revised the associated VSLs for Requirements R1 and R2 of CIP-003-7.
5. Revised the evidential language of Attachment 2 of CIP-003-7 by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to complement the revised requirement language.

Completed Actions	Date
Standard Authorization Request approved	July 20, 2016
Draft 1 of CIP-003-7(i) posted for formal comment and initial ballot	December 9, 2016 – January 23, 2017

Anticipated Actions	Date
10-day final ballot	February, 2017
NERC Board of Trustees adoption	February, 2017
Petition filed with FERC	March, 2017

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-7(i)

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. 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 SPS or RAS where the SPS or 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-003-7(i):

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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3. 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.

4.2.3.4. 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-003-7(i).

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation;

1.2.6. 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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1)	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1)	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the six topics required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 within 15 calendar	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the six topics required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 within 16 calendar	BES Cyber Systems, but did not address three of the six topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) 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 BES Cyber Systems 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	months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) 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 BES Cyber Systems 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	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.2)	calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2,	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing	to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but	access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR The Responsible Entity documented the determination of	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented	failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber	the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Assets and Removable Media, but 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 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2,		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 5.3. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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.	

Version	Date	Action	Change Tracking
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

Version	Date	Action	Change Tracking
			addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7(i)	TBD	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.

Attachment 1

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

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

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

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

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The

focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

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

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

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

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security

Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Rationale for Section 5 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

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

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

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

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, the use of one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;

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

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

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

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

Attachment 2

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

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

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

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

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

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

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

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

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

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability

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.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a

combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such

communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located

at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an “electronic boundary,” but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only “necessary” inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for “necessary” inbound and outbound electronic access controls may be documented within the Responsible Entity’s cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

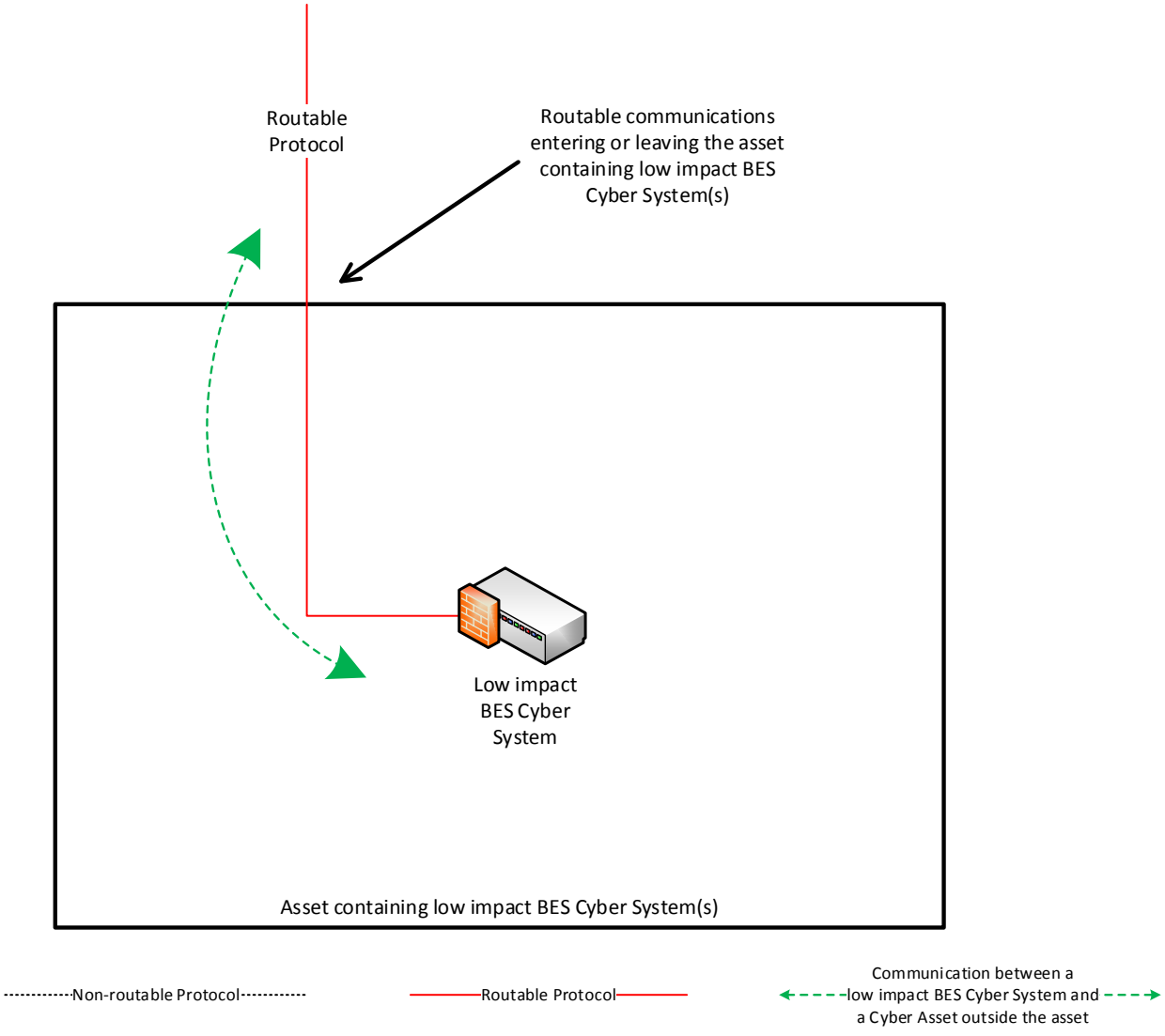
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

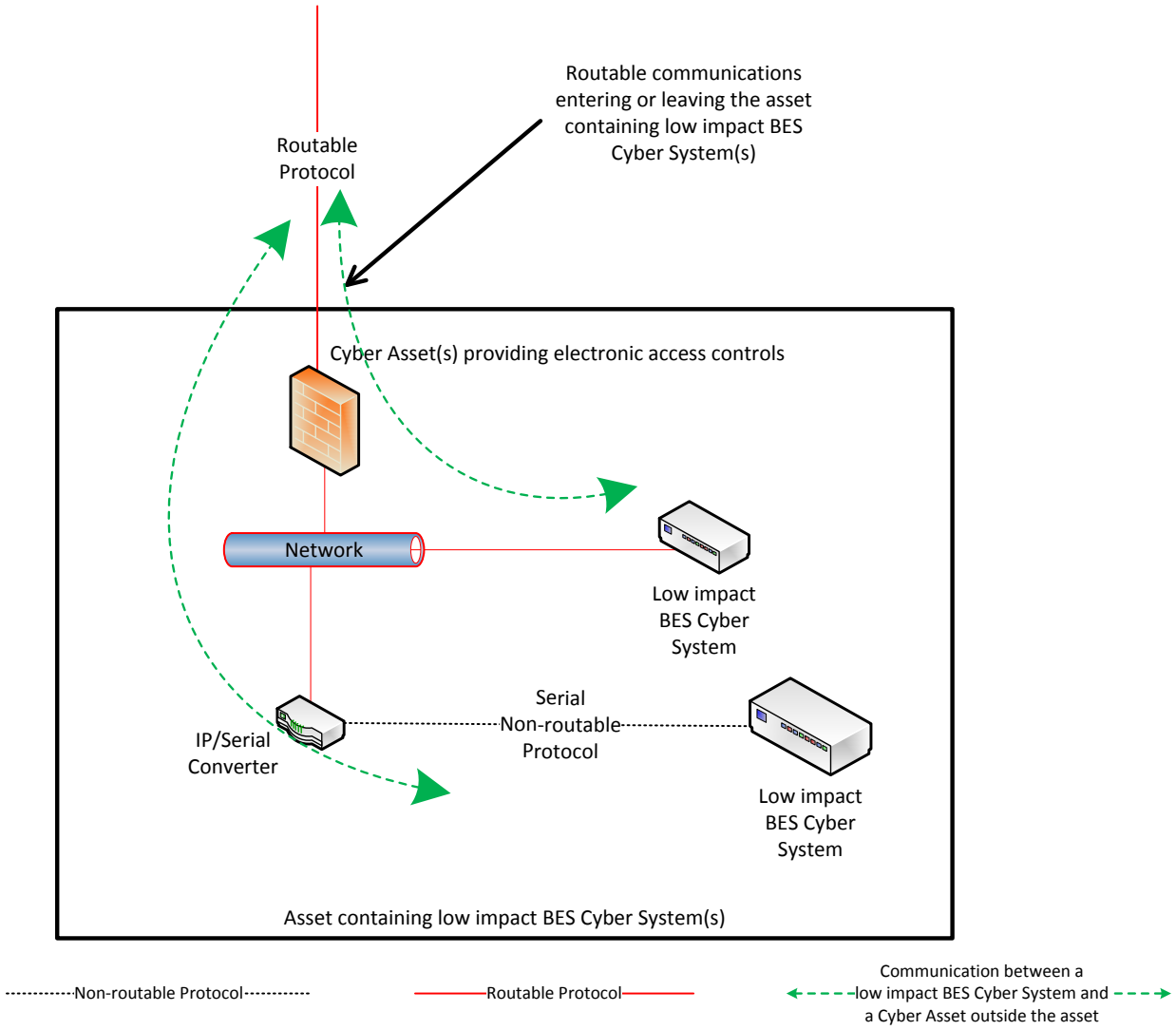
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

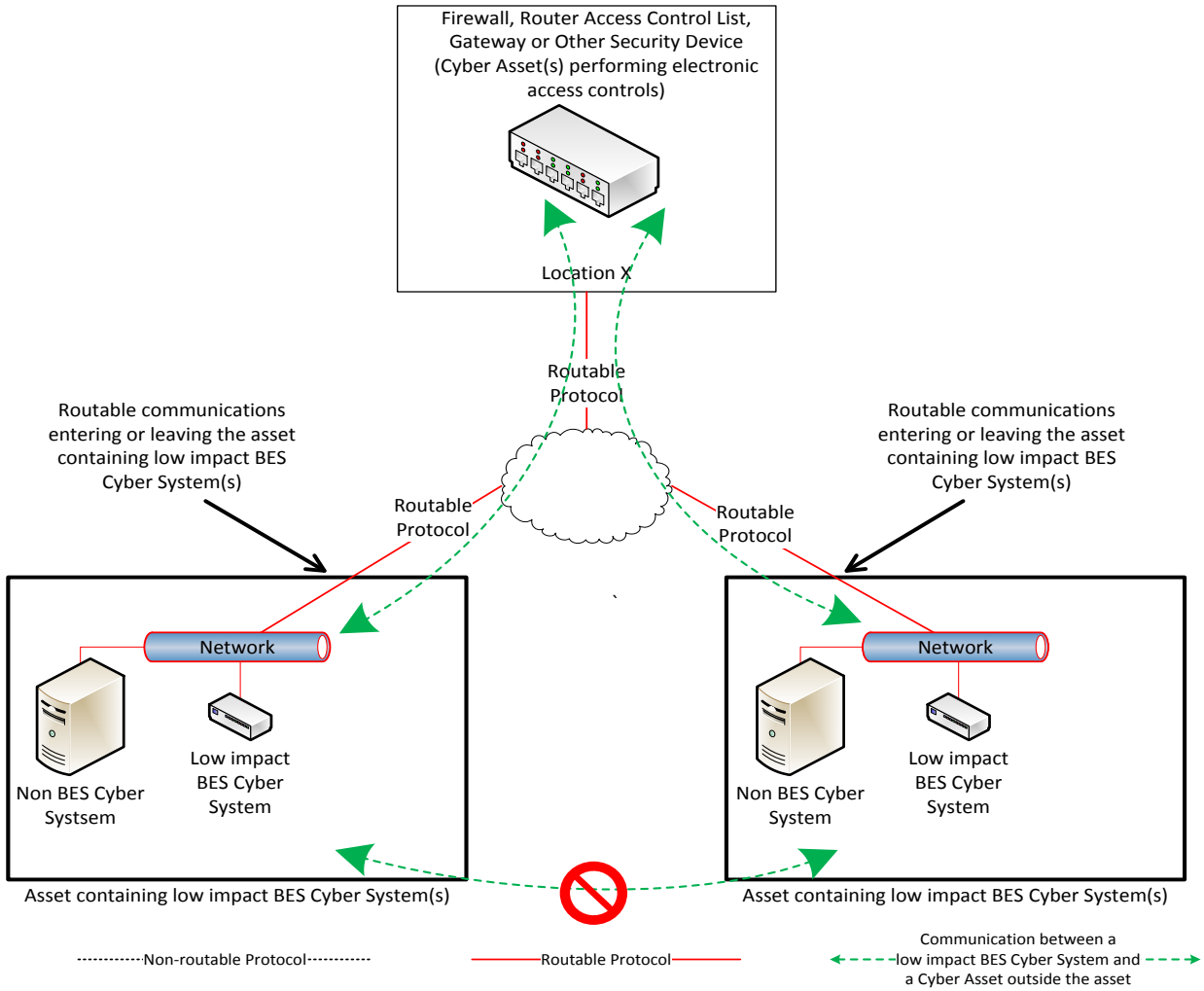
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

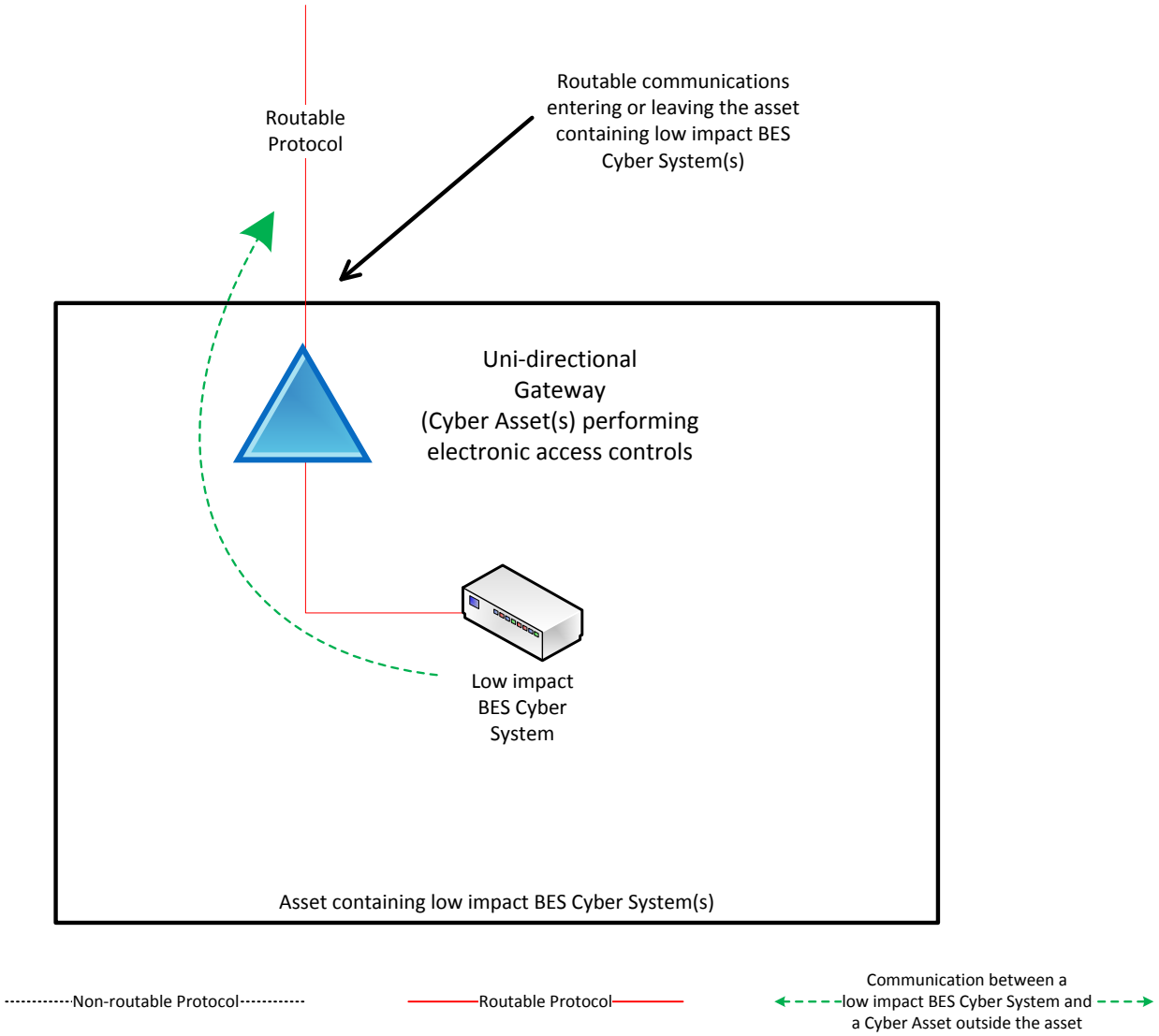
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

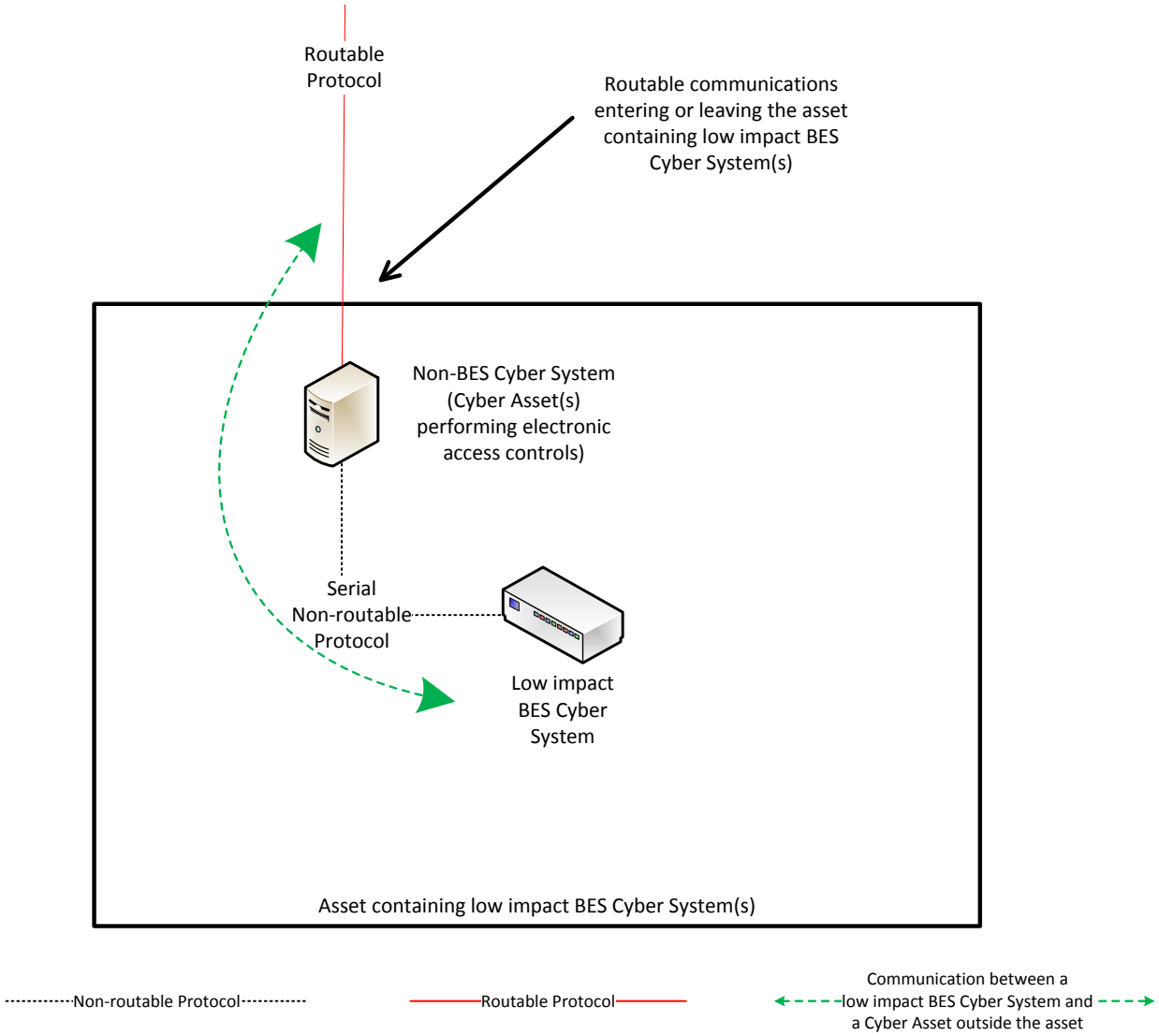
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

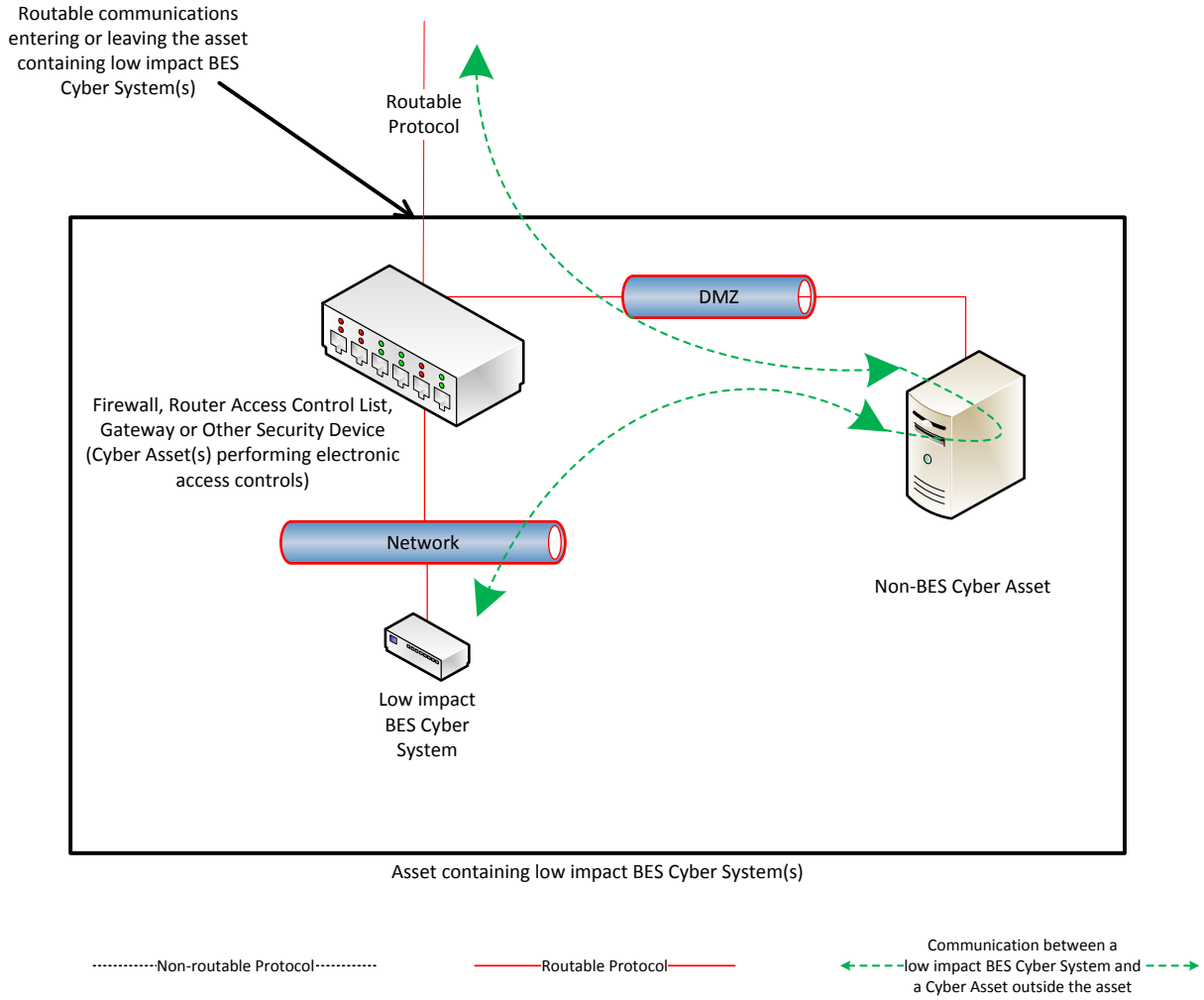
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

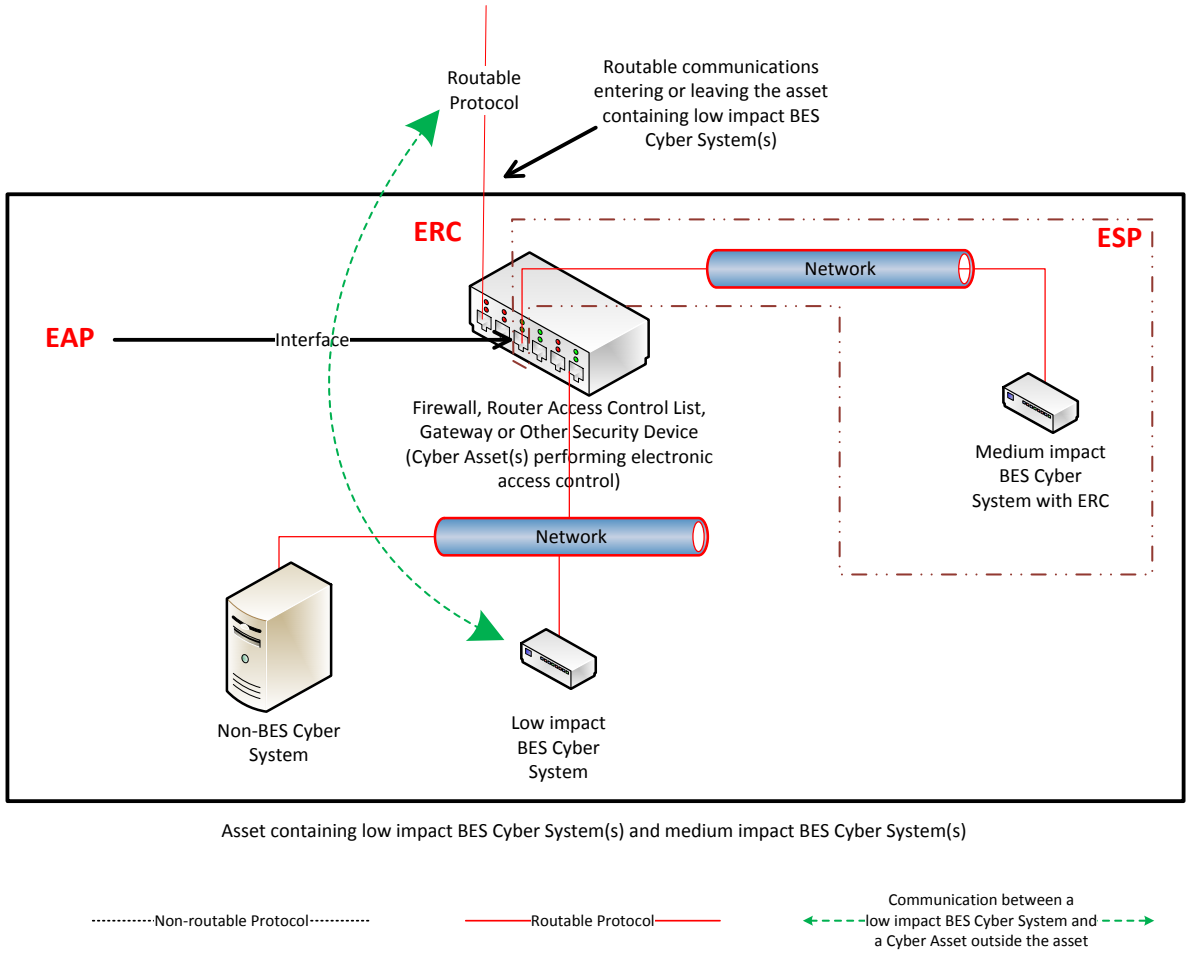
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.

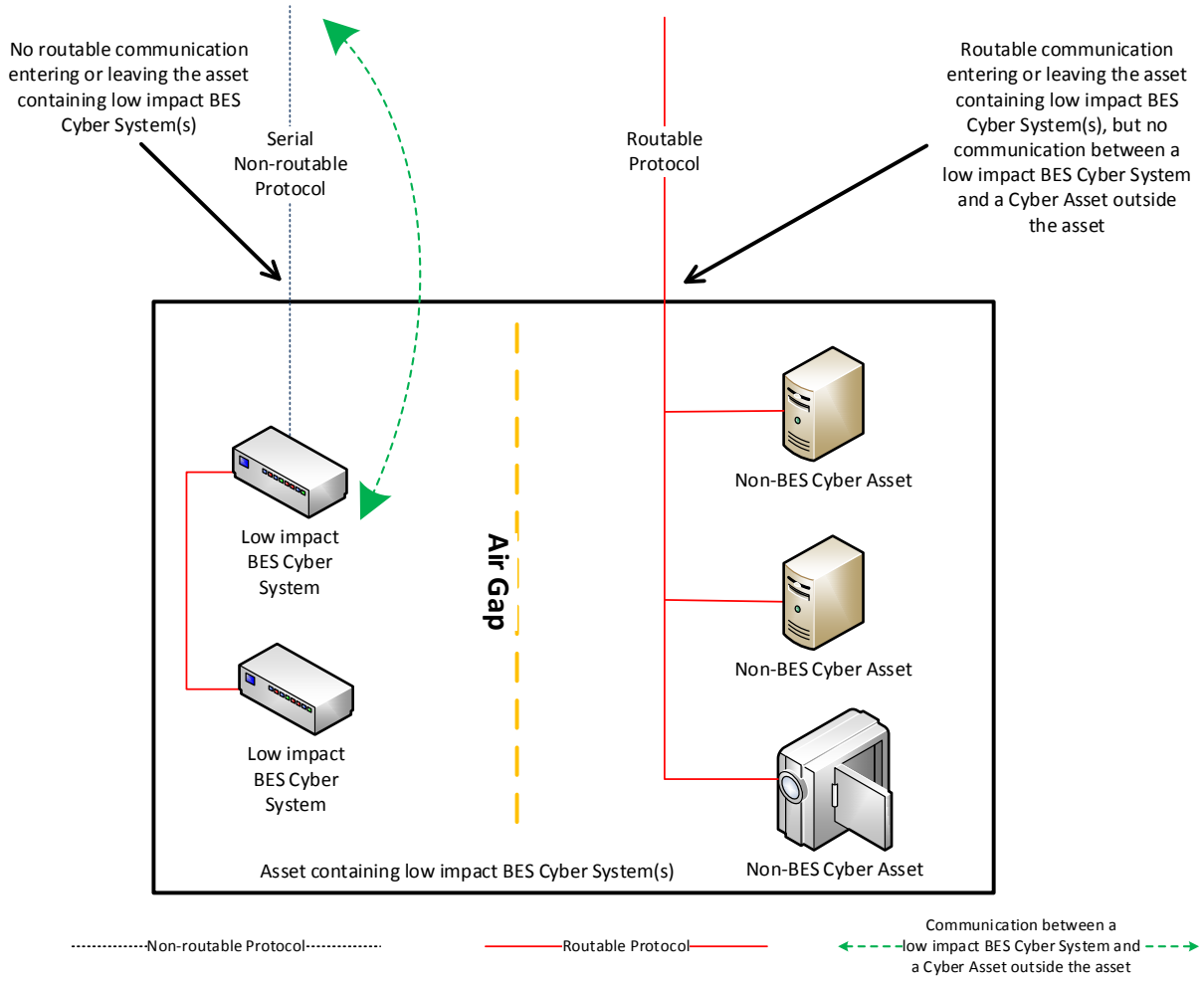


Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

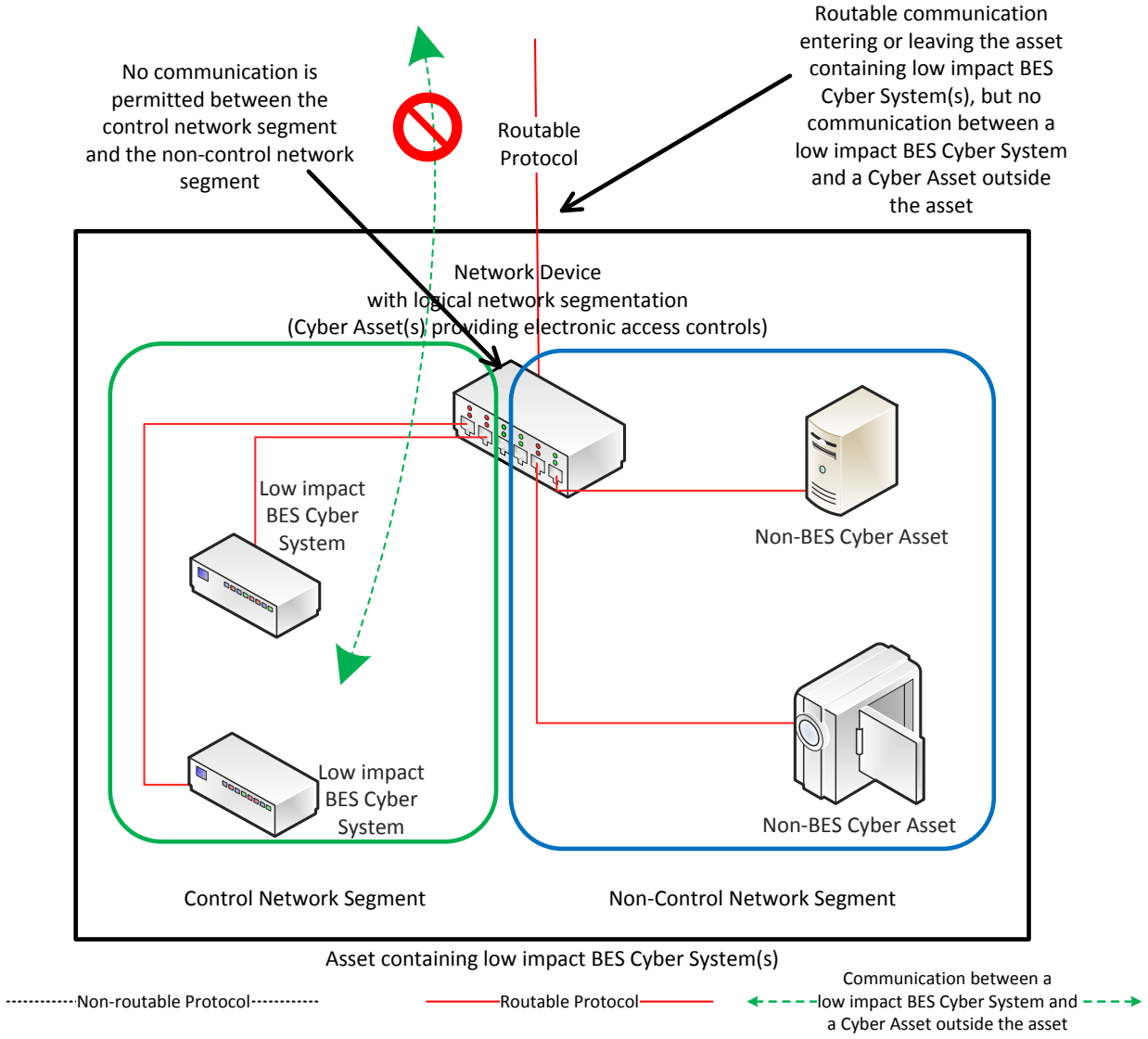
1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

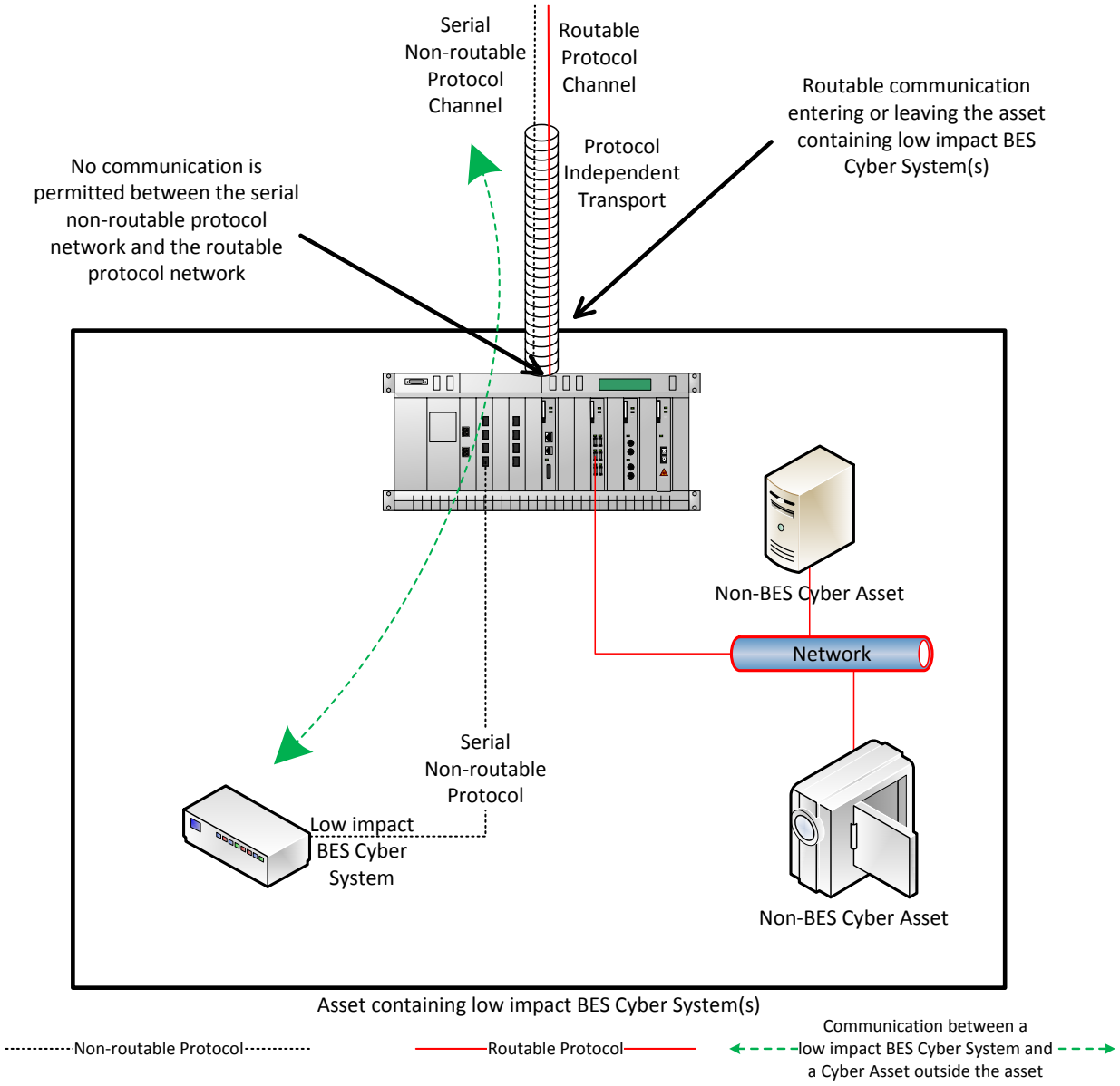
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Responsible Entiteis need Transient Cyber Assets and Removable Media to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices, including specially-designed devices for maintaining equipment in support of the BES or a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation in this context does not necessarily require that each vulnerability be individually addressed or remediated, as many vulnerabilities may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is intended to mean that entities take steps to reduce security risks presented by connecting the Transient Cyber Asset or Removable Media.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset. When addressing malicious code protection, Section 5.1 obligates the Responsible Entities to implement methods to mitigate the introduction of malicious code on Transient Cyber Assets managed by the Responsible Entity.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that

maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is some additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- If a Responsible Entity chooses touse methods that mitigate the introduction of malicious code other than those listed, it should documentat how the other method(s) meet the mitigation of the introduction of malicious code objective.

If malicious code is discovered, it must be mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect toTransiet Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. is the SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is

meeting the security objective. The intent is also not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party's and entity's actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This measure helps to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. However, the SDT does not intend for a Responsible Entity to conduct a review for every single connection of that Removable Media, but implement their process(es) in manner that protects all BES Cyber Systems where the Removable Media may be used. The intent is also not to require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated

the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives

the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for “clear lines of authority and ownership for security matters.” With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

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.

Description of Current Draft

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions to be incorporated into the Glossary of Terms Used in NERC Reliability Standards. In addition to approving the seven CIP Reliability Standards, the Commission, directed NERC to, among other things,: (1) "…develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems…", and (2) modify the definition of LERC.

In response to these directives, NERC first modified Reliability Standard CIP-003-6 to address the LERC directive, which has a regulatory deadline of March 31, 2017 for filing with the Commission. The revisions associated with the LERC directive were developed and posted for comment and ballot in July 2016 in draft Reliability Standard CIP-003-7. The revisions were not approved by stakeholders and based on the feedback received, the drafting team revised its approach and posted the revisions for an additional comment period and ballot. CIP-003-7 passed the additional ballot that ended on December 5, 2016.

For the transient device directive, NERC initially posted draft revisions for an informal comment period from November 1-18, 2016. This draft of Reliability Standard CIP-003-7(i) incorporates the proposed TCA language, as modified based on stakeholder comment, with the recently passed LERC revisions. The intent of this approach is to allow entities time to efficiently plan and implement the required modifications for low impact BES Cyber Systems. The Standard Drafting Team (SDT) approach to address the transient device directive is summarized below.

The SDT revised Attachment 1 of CIP-003-7 to include requirements that mitigate the risk to the BES of malware propagation from transient devices to low impact BES Cyber Systems. Attachment 1 contains and outlines the required sections of a Responsible Entity's cyber security plan(s) for its low impact BES Cyber Systems per Requirement R2. Previously, cyber security plan(s) were required to address four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. In keeping with the stakeholder approved approach to incorporate into one standard all the requirements applicable to assets containing low impact BES Cyber Systems, the SDT expanded CIP-003-7 Attachment 1 to include a fifth area: "Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation." Requiring the Responsible Entity to develop and implement these plans will provide higher assurance against the propagation of malware from transient devices.

In addition, the SDT determined it was necessary to revise the definitions of a Transient Cyber Asset (TCA) and Removable Media to ensure applicability of security controls and provide additional clarity. As well, the revised definitions accommodate use of the terms for all impact

levels: high, medium, and low. This is important for those entities that may opt to deploy one program to manage TCAs and Removable Media across multiple impact level assets.

The proposed revised definition of a Transient Cyber Asset (TCA) is:

A Cyber Asset that is:

1. *capable of transmitting or transferring executable code,*
2. *not included in a BES Cyber System,*
3. *not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and*
4. *directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:*
   - *BES Cyber Asset,*
   - *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
   - *PCA associated with high or medium impact BES Cyber Systems.*

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

The proposed revised definition of Removable Media is:

Storage media that:

1. *are not Cyber Assets,*
2. *are capable of transferring executable code,*
3. *can be used to store, copy, move, or access data, and*
4. *are directly connected for 30 consecutive calendar days or less to a:*
   - *BES Cyber Asset,*
   - *network within an Electronic Service Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
   - *Protected Cyber Asset associated with high or medium impact BES Cyber Systems.*

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

As proposed, Section 5 of Attachment 1 of CIP-003-7(i) mandates that entities have malware protection on TCAs (both entity and vendor-managed) and for Removable Media. The SDT proposes that it is necessary to distinguish between the specific protections for: (i) TCAs managed by the Responsible Entity, (ii) TCAs managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media.

For TCAs managed by the Responsible Entity, Section 5 requires the Responsible Entity to use one or a combination of the following to mitigate the introduction of malicious code: antivirus software, application whitelisting, or some other method. The SDT recognizes that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices (i.e., manage in an ongoing manner) while others have a checklist for transient devices prior to connecting them to a BES Cyber System (i.e., manage in an on-demand manner). The SDT acknowledges that both methods are effective and Section 5 permits either form of management. Because of the higher frequency in which these entity-managed devices are used, the controls required for these devices are more specific.

For Transient Cyber Assets managed by a party other than the Responsible Entity, Section 5 requires the Responsible Entity to review and verify the malware mitigation mechanism(s) used by the third party prior to connecting the Transient Cyber Asset (per Transient Cyber Asset capability).

For Removable Media, Section 5 requires entities to employ methods to detect malicious code and mitigate the threat of detected malicious code prior to connecting to a low impact BES Cyber System.

In summary, the SDT made the following changes to address the directive:

1. Revised the definitions of Transient Cyber Asset (TCA) and Removable Media.
2. Revised Requirement R1, by adding Parts 1.2.5 and 1.2.6 to include the complementary policies for the Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation in Requirement R2 (Attachment 1 of CIP-003-7(i)).
3. Revised the requirement language (Requirement R2) in Attachment 1 of CIP-003-7 by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation.
4. Revised the associated VSLs for Requirements R1 and R2 of CIP-003-7.
5. Revised the evidential language of Attachment 2 of CIP-003-7 by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to complement the revised requirement language.

Completed Actions	Date
Standard Authorization Request approved	July 20, 2016
Draft 1 of CIP-003-7(i) posted for formal comment and initial ballot	December 9, 2016 – January 23, 2017

Anticipated Actions	Date
10-day final ballot	February, 2017
NERC Board of Trustees adoption	February, 2017
Petition filed with FERC	March, 2017

A. Introduction

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

2. **Number:** CIP-003-~~6~~7(i)

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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. Interchange Coordinator or Interchange Authority

   4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. 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 SPS or RAS where the SPS or 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-~~6:~~ 7(i):

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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3. 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.

4.2.3.4. 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-~~6.~~7(i).

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls ~~for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and~~;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation;

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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None.

2. Table of Compliance Elements

~~R~~ #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7 (i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the ~~four~~six topics required by R1. (R1.2) 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 BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the ~~four~~six topics required by R1. (R1.2) 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 BES Cyber Systems as	BES Cyber Systems, but did not address three of the ~~four~~six topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address ~~any~~four or more of the ~~four~~six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	Systems as required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but	The Responsible Entity failed to document ~~or~~and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to ~~CIP-003-6,~~ Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident	containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented	failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2,	its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response ~~plans~~plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for	The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~E-ISAC) according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented ~~and implemented electronic access controls~~its plan(s) for ~~LERC~~Transient Cyber Assets and Removable Media, but failed to implement ~~a LEAP or permit inbound and outbound access~~ mitigation for the	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	identification, classification, and response to Cyber Security Incidents according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) ~~-~~OR ~~(R2)~~ ~~OR~~ The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent	introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section ~~3~~5.1. (R2) OR The Responsible Entity documented ~~and implemented electronic access controls~~its plan(s) for ~~its assets containing low impact BES~~Transient Cyber ~~Systems~~Assets and Removable Media, but failed to ~~document and~~ implement ~~authentication of all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems~~mitigation for the introduction of malicious code for Transient Cyber Assets	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				notification to the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~E-ISAC) according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its ~~cyber security~~ plan(s) for ~~its assets containing low impact BES~~Transient Cyber ~~Systems~~Assets and Removable Media, but failed to document ~~physical security controls~~ mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible	managed by a party other than the Responsible Entity according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, Section ~~3~~5.2. (R2) OR The Responsible Entity documented ~~the physical access controls~~its plan(s) for ~~its assets containing low impact BES~~Transient Cyber ~~Systems~~Assets and Removable Media, but failed to implement ~~the physical security controls~~mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to ~~CIP-003-6,~~ Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Entity according to ~~CIP-003-6,~~ Requirement R2, Attachment 1, ~~Section 2.~~ Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its ~~cyber security~~ plan(s) for ~~its assets containing low impact BES~~Transient Cyber ~~Systems~~Assets and Removable Media, but failed to document ~~electronic access controls~~mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to ~~CIP-003-6,~~Requirement	Attachment 1, Section ~~2~~5.3. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			40 calendar days of the change. (R3)	change in less than 50 calendar days of the change. (R3)		Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but 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. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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.	

Version	Date	Action	Change Tracking
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 devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	

~~CIP-003-6 -~~

7(i)	TBD	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.

Attachment 1

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

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

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

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

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that

provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

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

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

Section 3. ~~For LERC, if any,~~ implement ~~a LEAP to permit~~electronic access controls to:

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

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

~~i.~~ii. using a routable protocol ~~access;~~when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. ~~Implement authentication for~~not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity ~~Sector~~ Information Sharing and Analysis Center (~~ES~~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.

~~CIP-003-6 -~~

Rationale for Section 5 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

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

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

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

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, the use of one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or

- Other method(s) to mitigate the introduction of malicious code.

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

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

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

Attachment 2

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

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

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

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

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

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

1. Documentation showing that ~~inbound and outbound connections for any LEAP(s) are confined to only those the Responsible Entity deems necessary (e.g., by restricting IP addresses, ports, or services); and documentation~~at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of

implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

~~1.~~2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

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

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or

system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability

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.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-~~6~~7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-~~6~~7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the ~~four~~six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-~~6~~7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts

- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

~~Using the list of assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement~~The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that ~~addresses~~address the security objective ~~criteria~~ for the protection of low impact BES Cyber Systems. ~~The protections required by Requirement R2 reflect the level of risk that misuse or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the~~The required protections are designed to

be part of a program that covers the low impact BES Cyber Systems collectively ~~either~~ at an asset ~~or site~~ level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

~~There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and Dial-up Connectivity, and (4) Cyber Security Incident response.~~

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the ~~four~~ subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible ~~Entity is not~~Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems ~~at assets containing low impact BES Cyber System(s)~~ within the asset, and (2) ~~LEAPs~~Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If ~~the LEAP is~~these Cyber Assets implementing the electronic access controls are located within the ~~BES asset and inherits the~~ same ~~controls~~ asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this ~~can~~may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility ~~in the selection of~~to select the methods used to meet the objective ~~to control~~ of controlling physical access to (1) the asset(s) containing low impact BES Cyber ~~Systems,~~System(s) or the low impact BES Cyber Systems themselves~~, or LEAPs~~ and (2)

the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level for access to the site or systems, including LEAPs.. The requirement doesstandard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of a useran individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). TheThe standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of boundary protectionselectronic access controls for assets containing low impact BES Cyber Systems when the low impact BES Cyber Systems have bi-directionalthere is routable protocol communication or Dial-up Connectivity to devices external to between Cyber Asset(s) outside of the asset containing the low impact BES Cyber Systems. The establishment of boundary protections is intended to control communication either into the asset containing low impact BES Cyber System(s) or toand the low impact BES Cyber System itself to (s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. The term "electronic access control" is used in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing. The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or **Dial-up Connectivity** present. In the case where there is no external bi-directional routable protocol communication, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s).

The defined terms LERCWhen implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and LEAPoutbound electronic access are used to avoid confusion with the similar terms

~~used~~required for ~~high~~communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and ~~medium~~when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems ~~(e.g., External Routable~~that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity ~~(ERC) or~~ to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access ~~Point (EAP)). To future-proof the standards, and in~~Control Exclusion

In order to avoid future technology issues, the ~~definitions specifically~~obligations for electronic access controls exclude ~~"point-to-point~~ communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions ~~between Transmission station or substation assets containing low impact BES Cyber Systems,",~~ such as IEC TR-61850-90-5 R-GOOSE messaging. ~~This does not exclude Control Center communication but rather excludes the communication between the intelligent electronic devices themselves.~~Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement ~~a LEAP.~~the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive ~~requirements~~characteristics related to this

technology ~~nor~~and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

~~When determining whether~~ **Considerations for Determining Routable Protocol Communications**

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is ~~LERC to the low impact BES Cyber System, the definition uses the phrases "direct user-initiated interactive access or a direct device-to-device connection to~~ communication between a low impact BES Cyber System(s) ~~from~~and a Cyber Asset(s) outside the asset containing ~~those~~the low impact BES Cyber System(s) ~~via~~that uses a routable protocol when entering or leaving the asset.

When determining whether a ~~bi-directional~~ routable protocol ~~connection." The intent of "direct" in the definition~~ is ~~to indicate LERC exists if a person is sitting at another device outside of~~entering or leaving the asset containing the low impact BES Cyber System~~, and~~ (s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the ~~person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session even if there is a serial-to-~~routable protocol ~~conversion. The reverse case would also be LERC, in which the individual sits at the~~communication entering or leaving the asset between a low impact BES Cyber System and ~~connects~~ Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to ~~a device~~ be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber ~~Systems using a single end-to-end bi-directional routable protocol session. Additionally, for "device to~~ System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and

implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

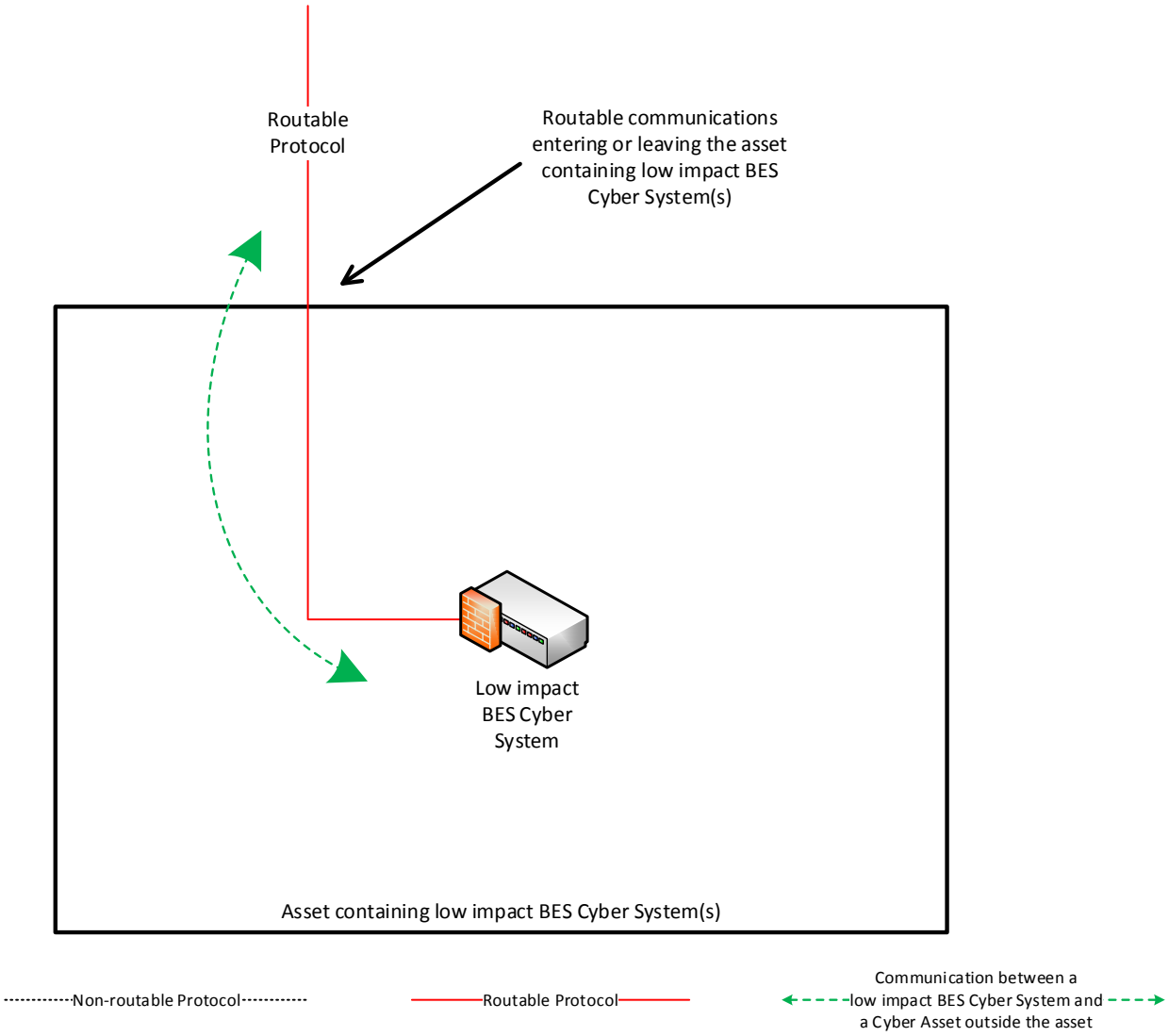
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

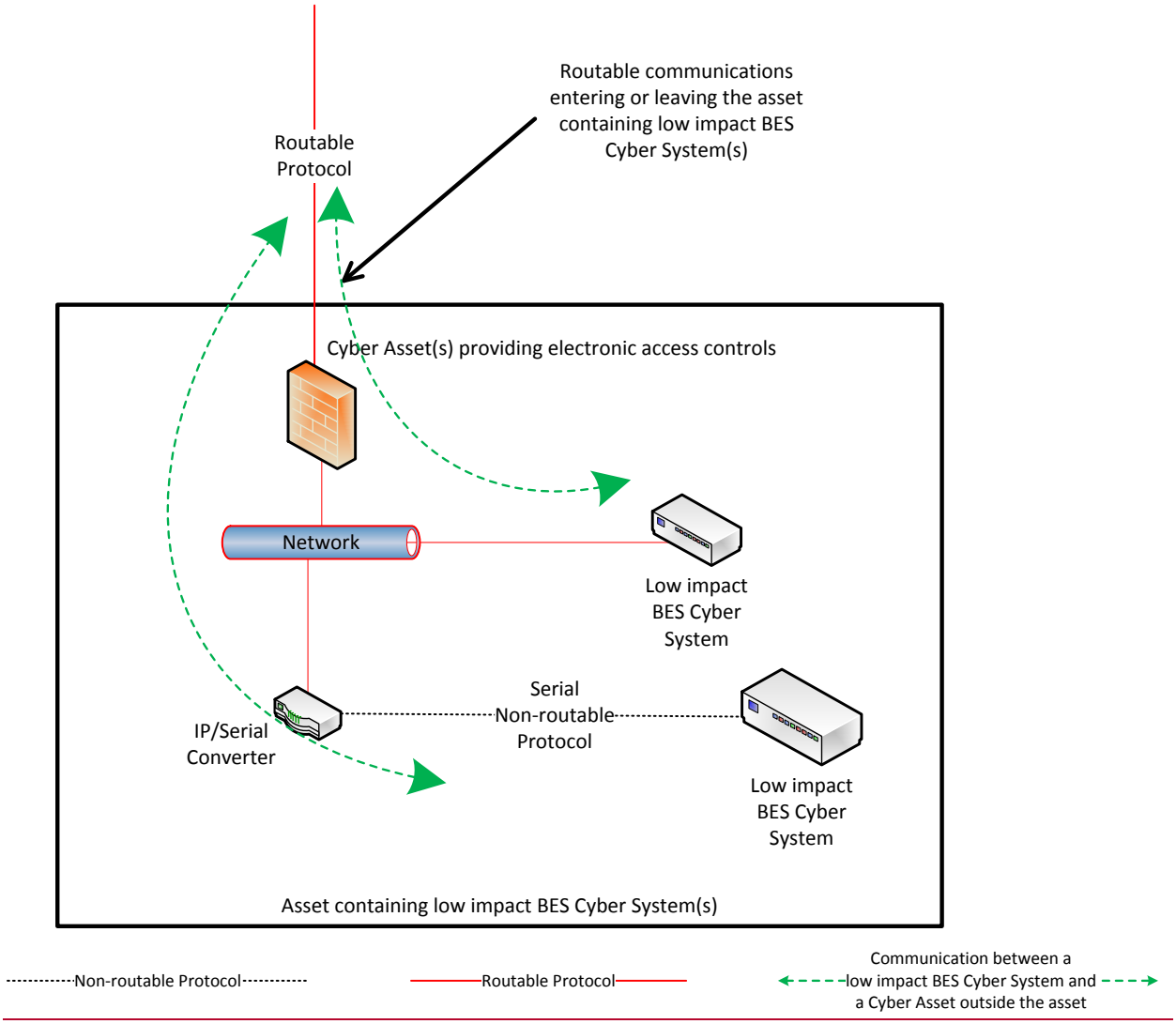
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

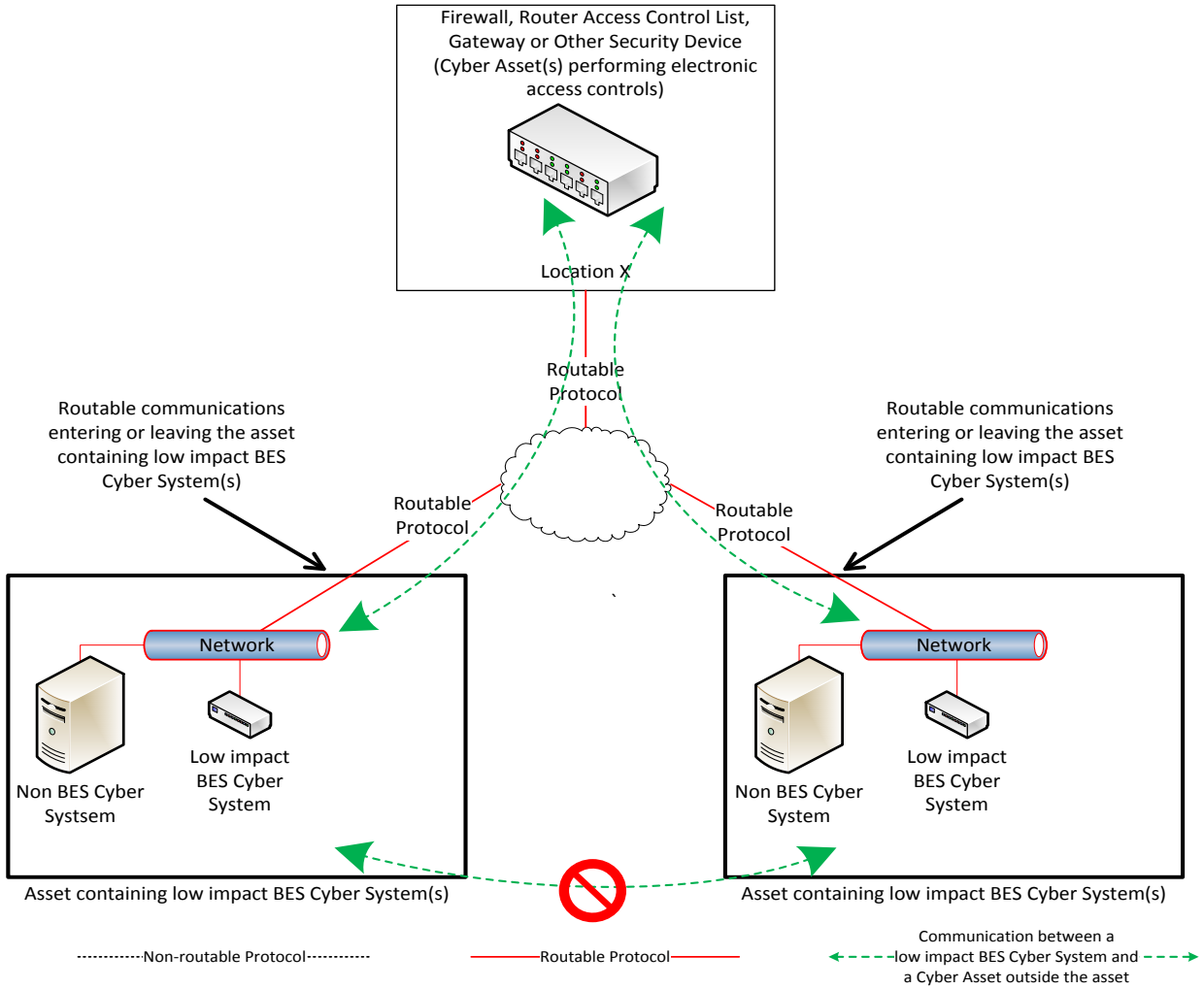
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

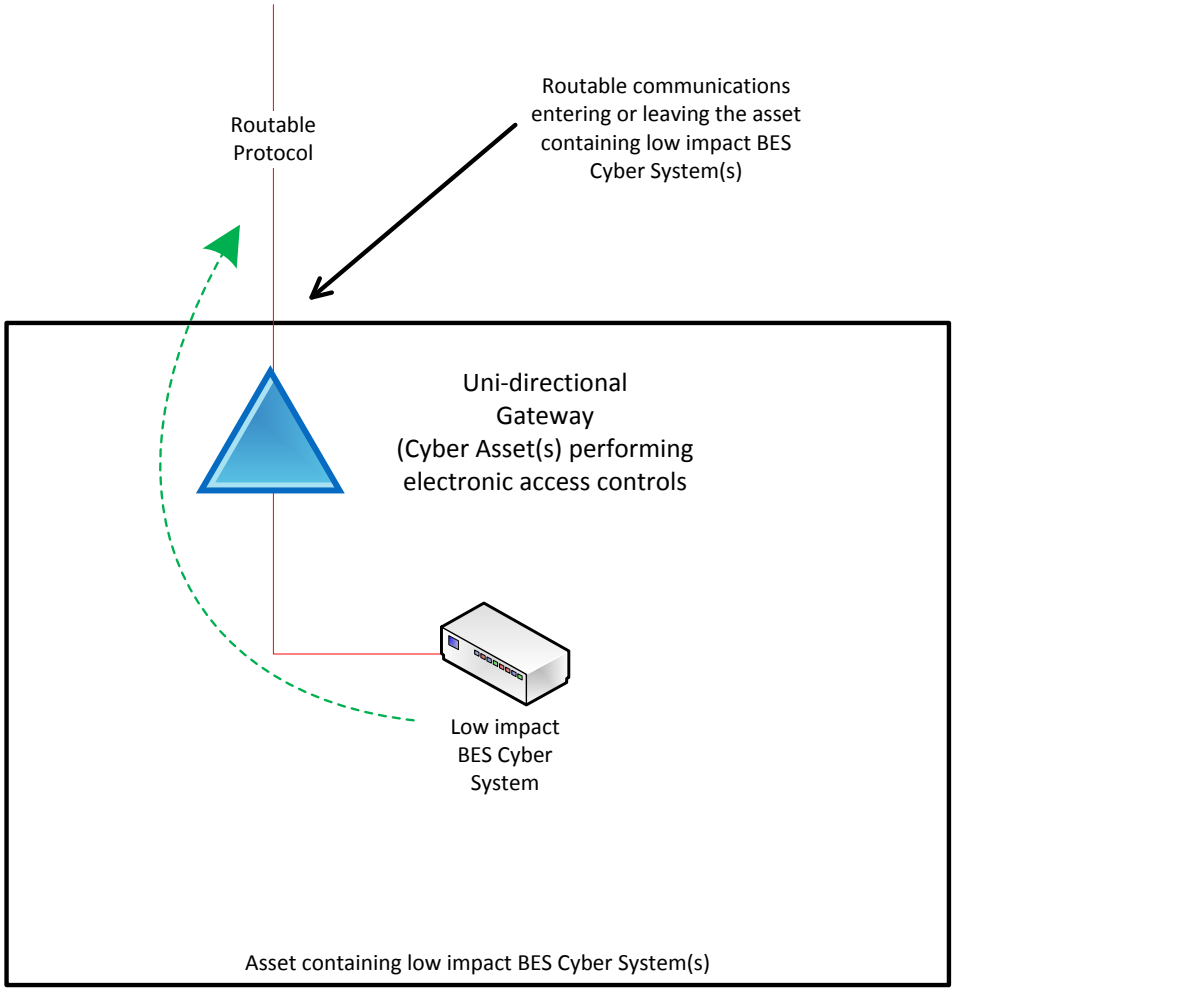
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

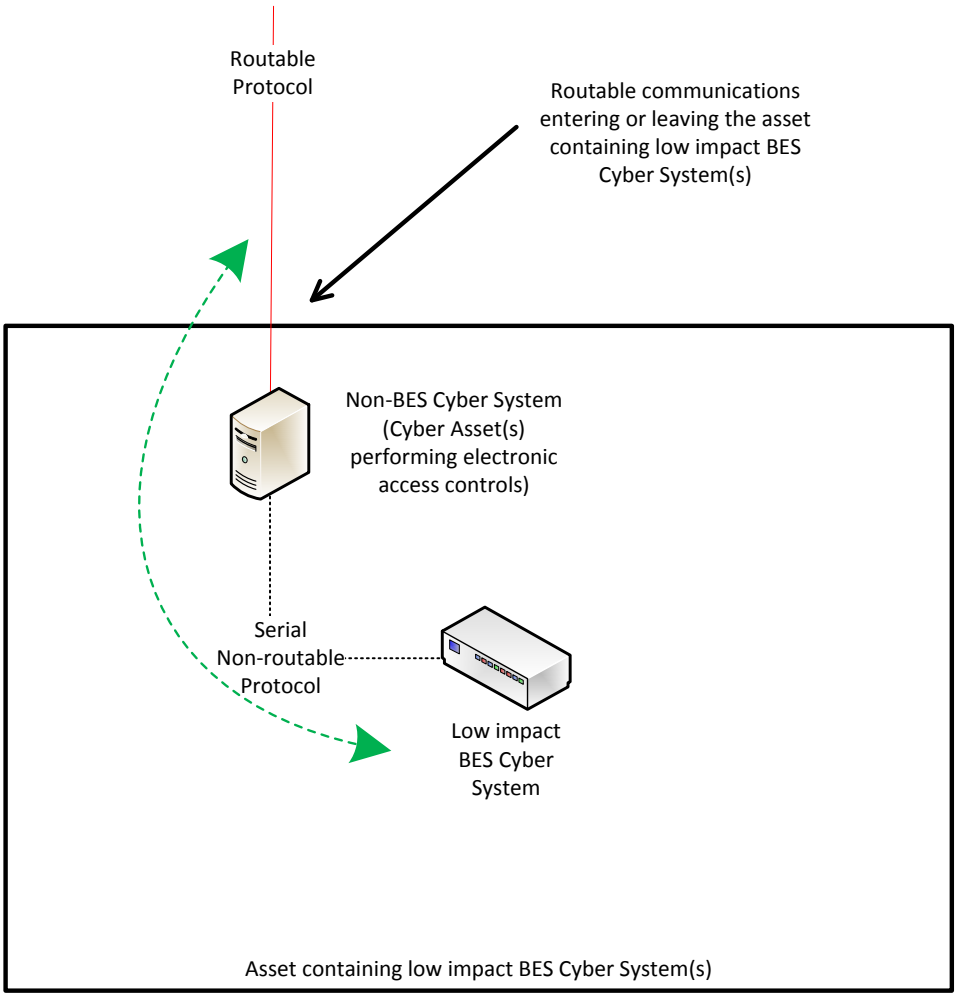
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

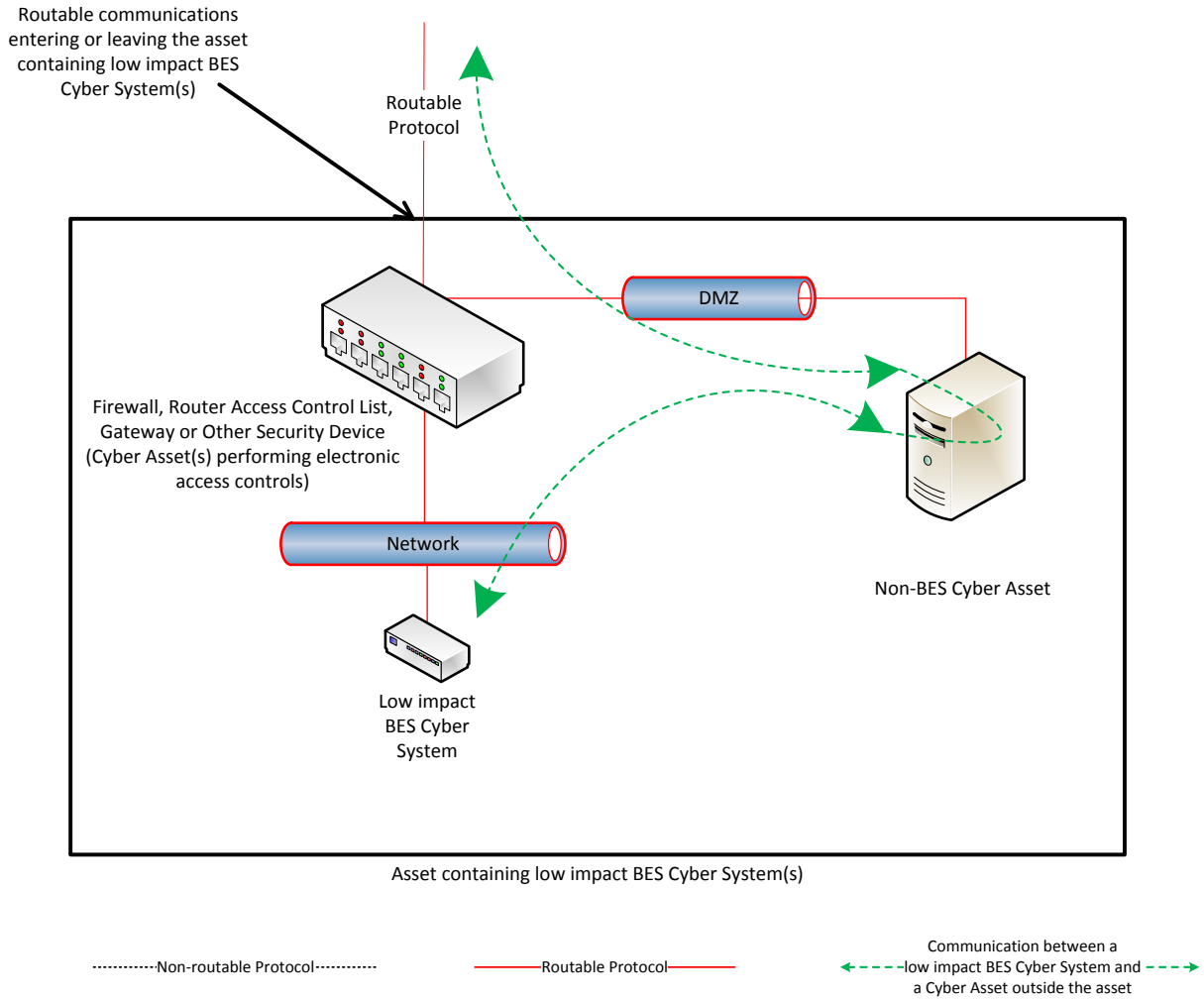
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

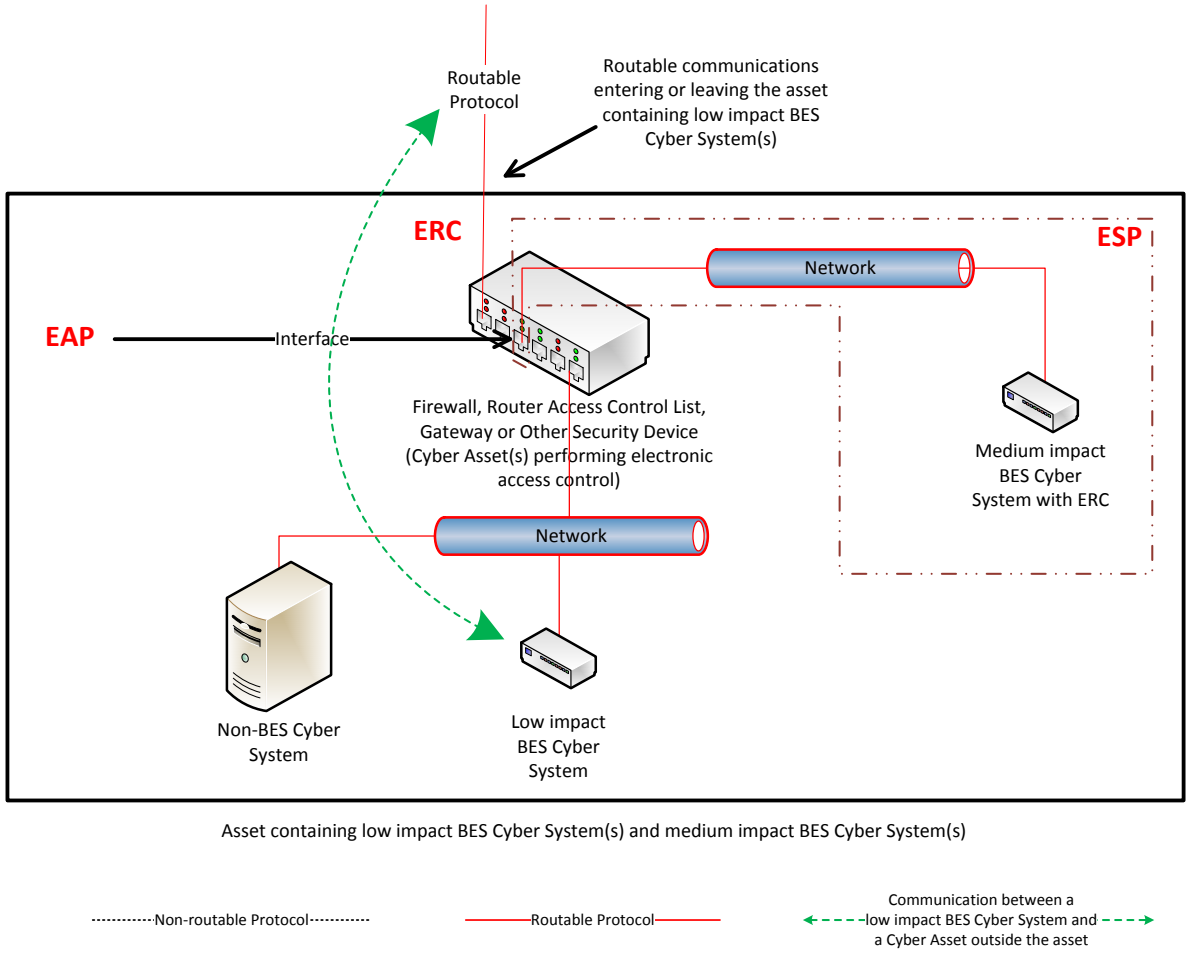
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device ~~connection," LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication to or from the low impact BES Cyber System.~~ that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.

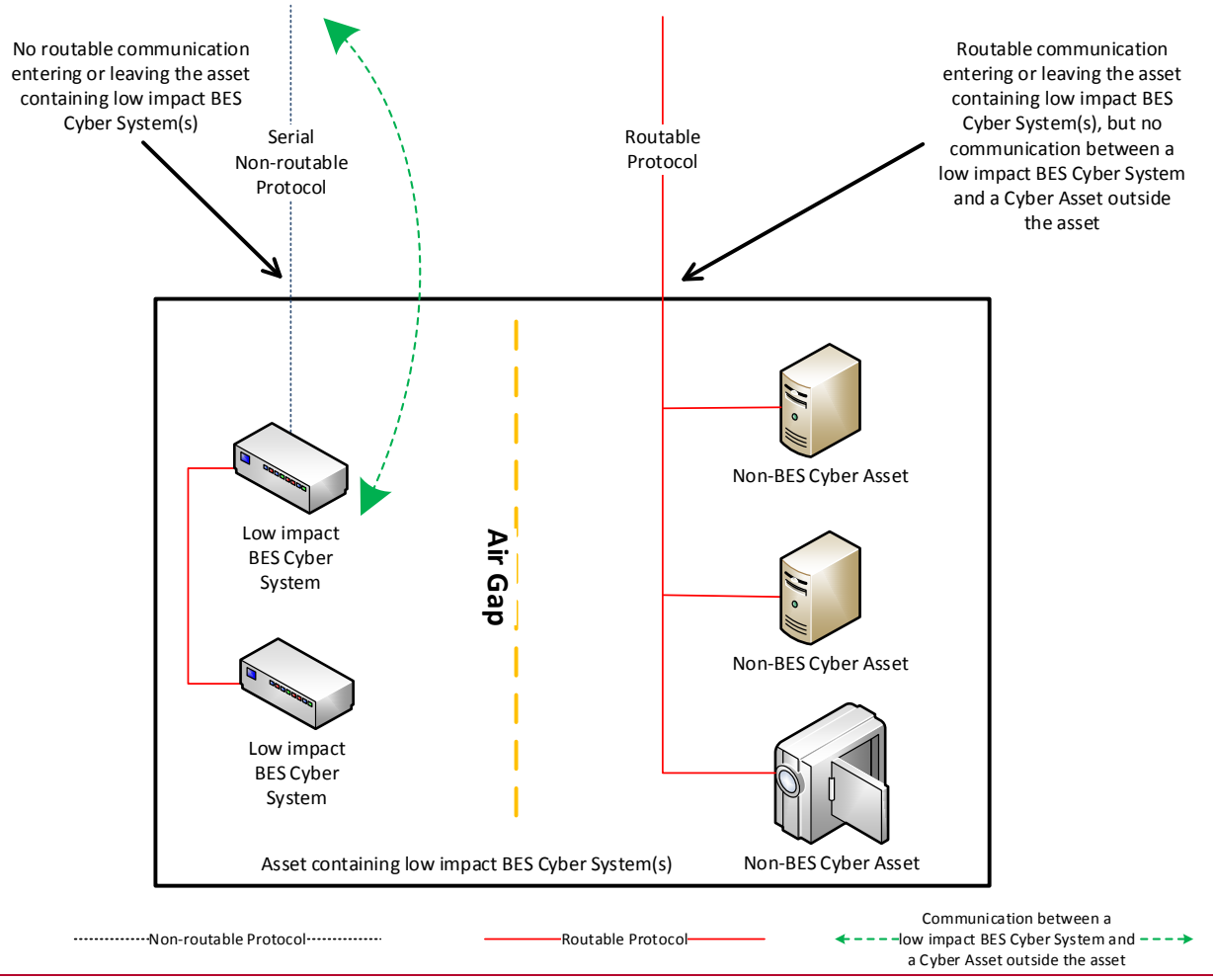


Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

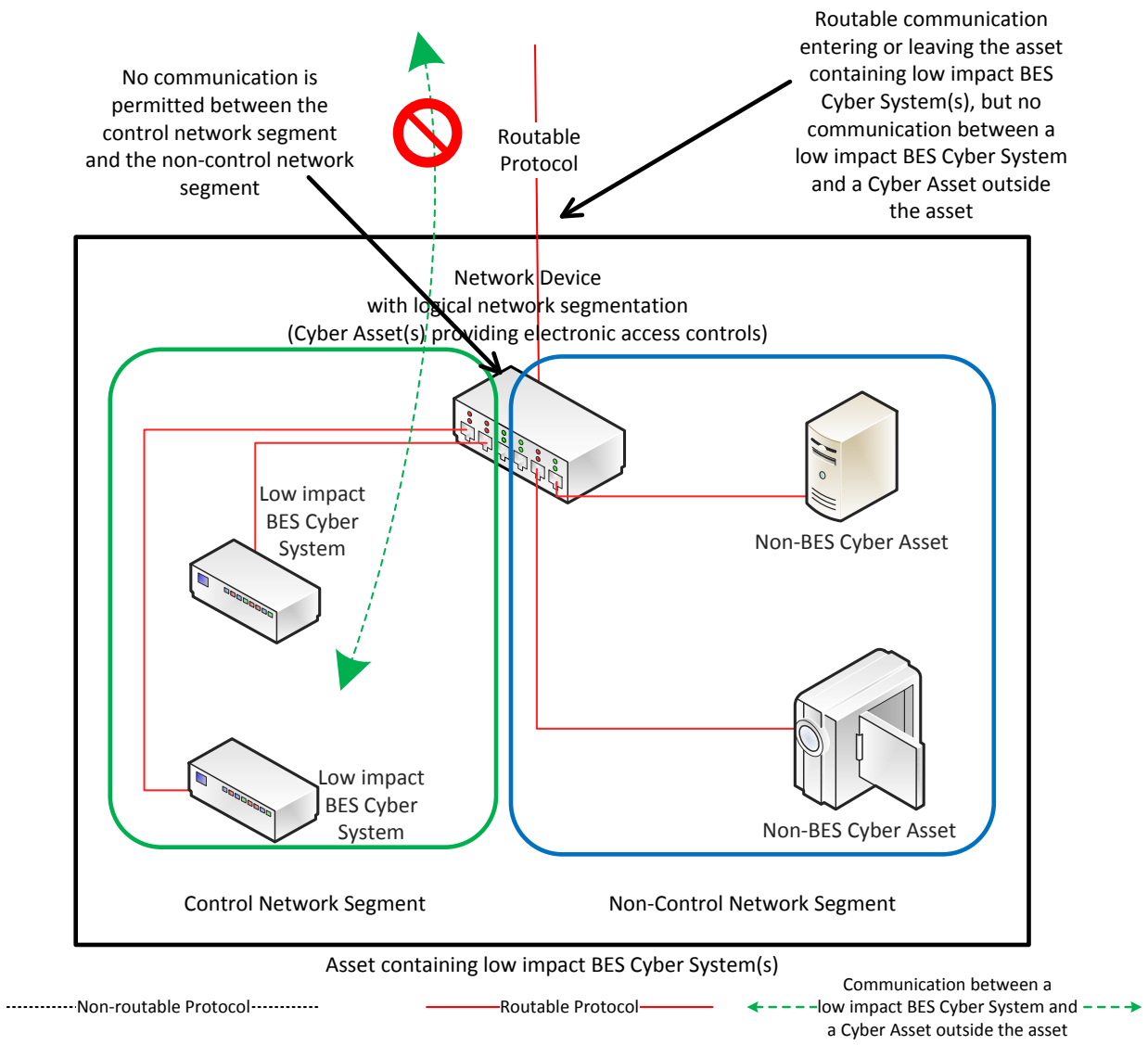
1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

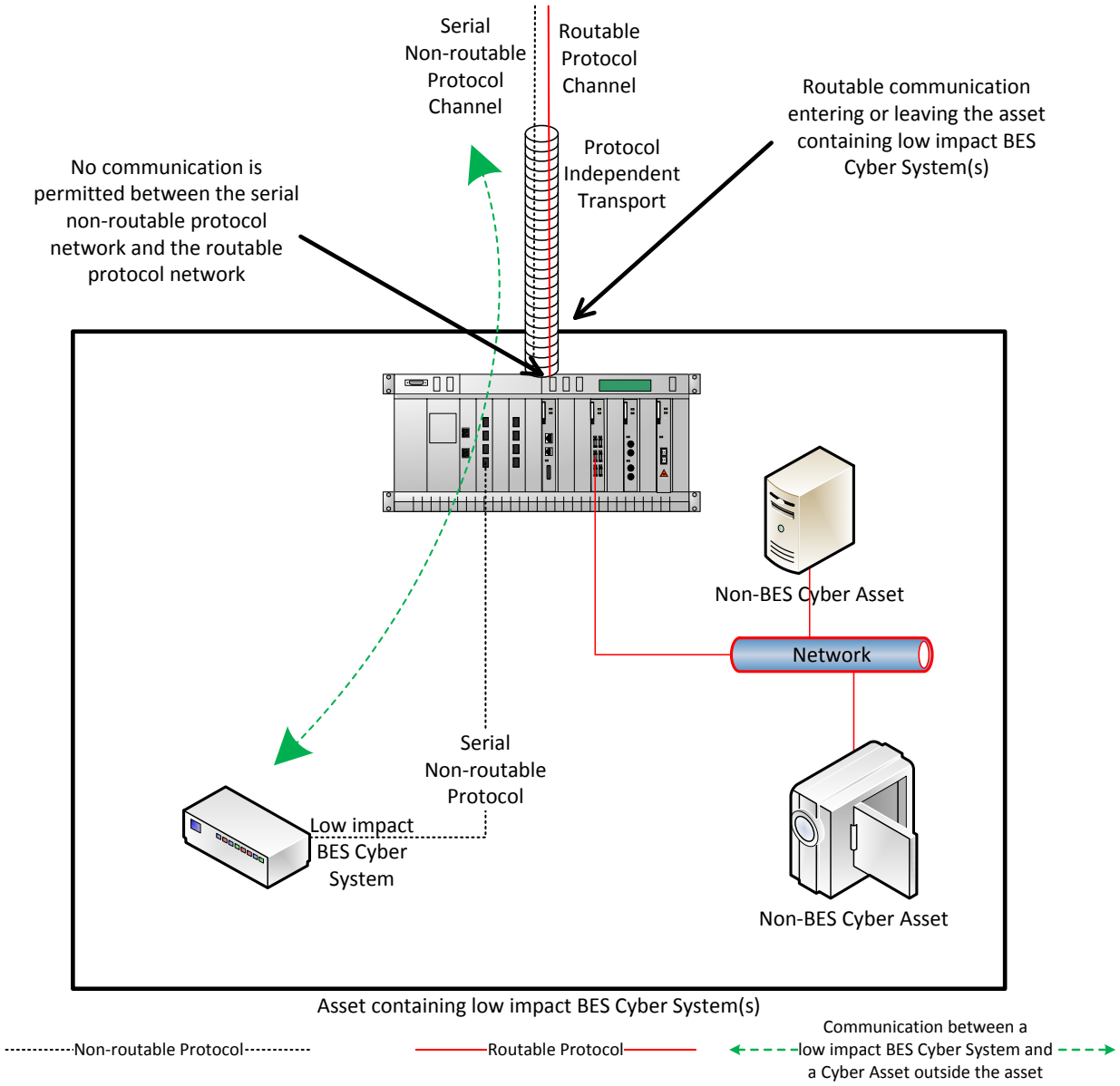
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity When identifying a LEAP, Responsible Entities are provided flexibility in the selection of the interface on a Cyber Asset that controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, the internal interface on a router that has implemented an access control list (ACL), or other security device. The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required to reside at the asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP per asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber Systems. Locating the Cyber Asset with multiple LEAPs at an external location with multiple assets containing low impact BES Cyber Systems "behind" it, however, should not allow uncontrolled access to assets containing low impact BES Cyber Systems sharing a Cyber Asset containing the LEAP(s).

In Reference Model 4, the communication flows through an IP/Serial converter. LERC is correctly identified in this Reference Model because the IP/Serial converter in this instance is doing nothing more than extending the communication between the low impact BES Cyber System and the Cyber Asset outside the asset containing the low impact BES Cyber System. In contrast, Reference Model 6 has placed a Cyber Asset that performs a complete break or interruption that does not allow the user or device data flow to directly communicate with the low impact BES Cyber System. The Cyber Asset in Reference Model 6 is preventing extending access to the low impact BES Cyber System from the Cyber Asset outside the asset containing the low impact BES Cyber System. The intent is that if the IP/Serial converter that is deployed only does a "pass-through" of the data flow communication, then that "pass-through" data flow communication is LERC and a LEAP is required. However, if that IP/Serial converter performs some type of authentication in the data flow at the asset containing the low impact BES Cyber System before the communication can be sent to the low impact BES Cyber System, then that type of IP/Serial converter implementation is not LERC.

A Cyber Asset that contains interface(s) that only perform the function of a LEAP does not meet the definition of Electronic Access Control or Monitoring System (EACMS) associated with medium or high impact BES Cyber Systems and is not subject to the requirements applicable to an EACMS. However, a Cyber Asset may contain some interfaces that function as a LEAP and other interfaces that function as an EAP for high or medium impact BES Cyber Systems. In this case, the Cyber Asset would also be subject to the requirements applicable to the EACMS associated with the medium or high impact BES Cyber Systems.

Examples of sufficient access controls may include:

- Any LERC for the asset passes through a LEAP with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g., IP addresses, ports, or services).
- As shown in Reference Model 1 below, the low impact BES Cyber System has a host-based firewall that is controlling the inbound and outbound access. In this model, it is also possible that the host-based firewall could be on a non-BES

Cyber Asset. The intent is that the host-based firewall controls the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in the business network.

- As shown in Reference Model 5 below, a non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that the non-BES Cyber Asset has provided a "protocol break" so that access to the low impact BES Cyber System is only from the non-BES Cyber Asset that is located within the asset containing the low impact BES Cyber System.

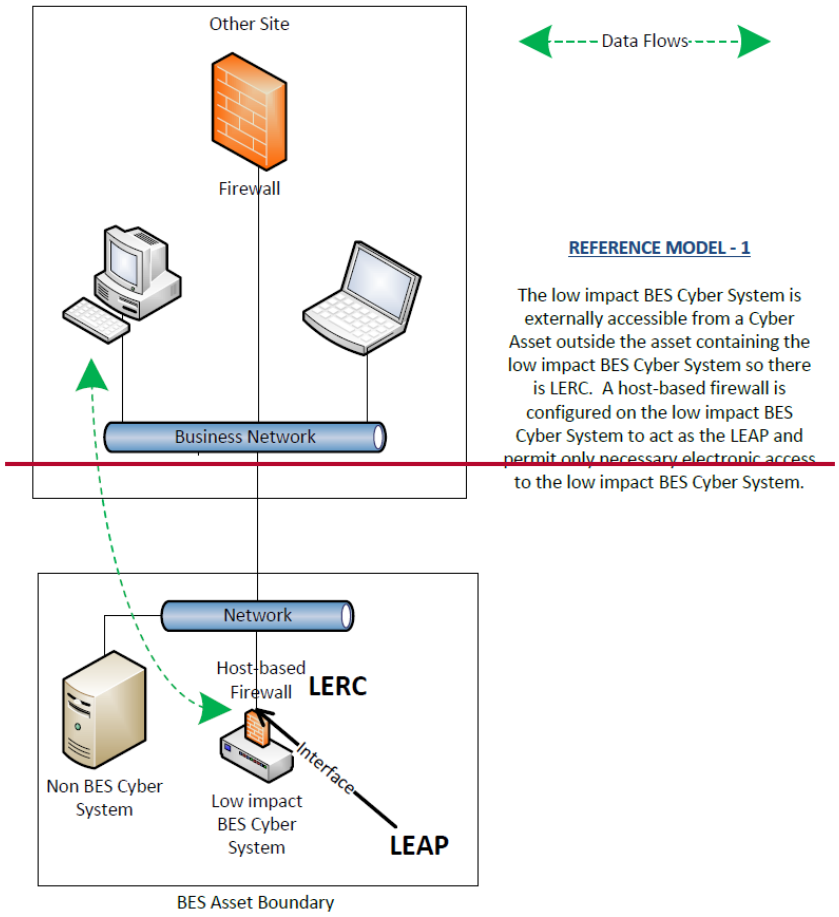
Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

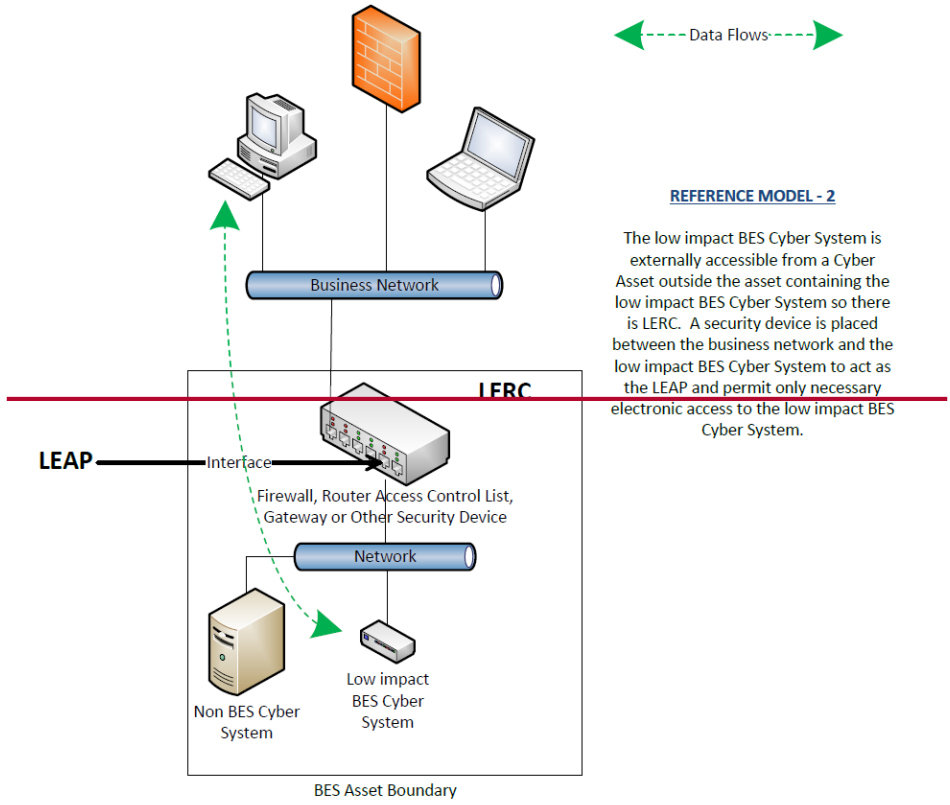
- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- An asset has LERC due to aA low impact BES Cyber System within it havinghas a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- In Reference Model 5, using just dualDual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the businessexternal network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devicedevices on thatthe non-BES Cyber Asset.

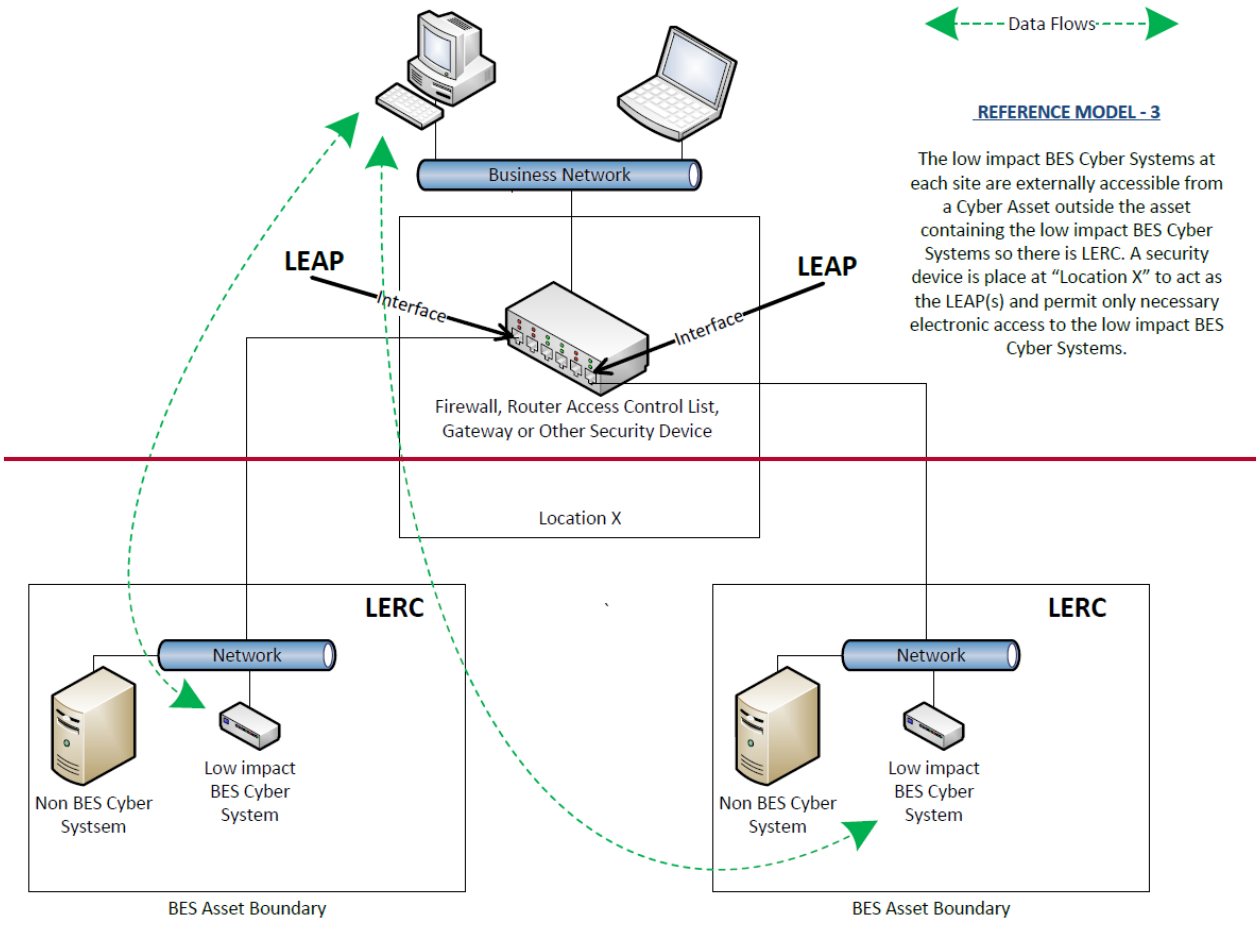
The following diagrams provide reference examples intended to illustrate how to determine whether there is LERC and for implementing a LEAP. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.

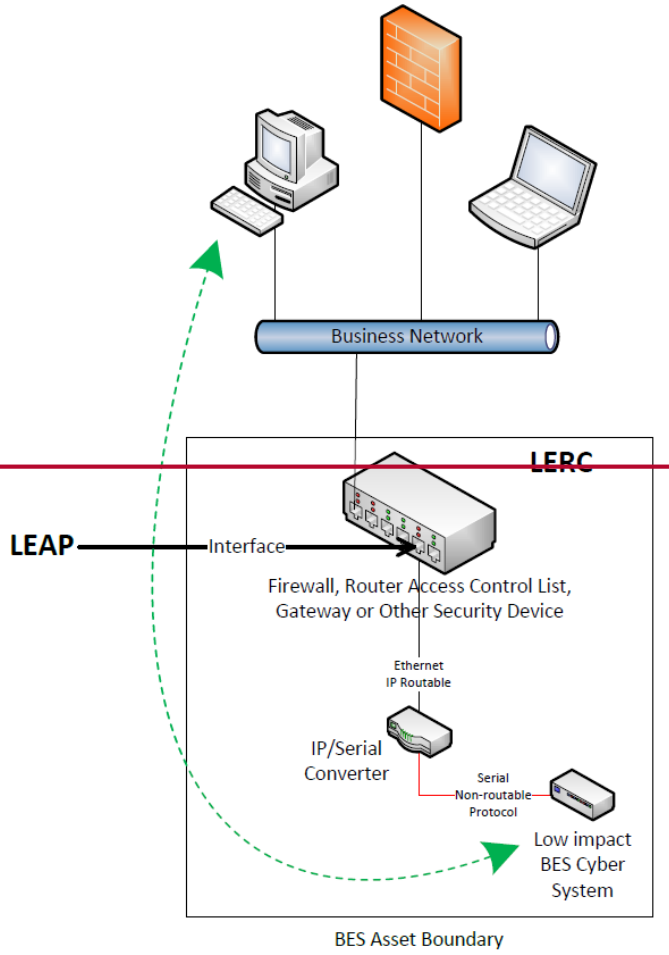


REFERENCE MODEL - 1

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A host-based firewall is configured on the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.


Data Flows
REFERENCE MODEL - 2
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.
Business Network
LERC
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

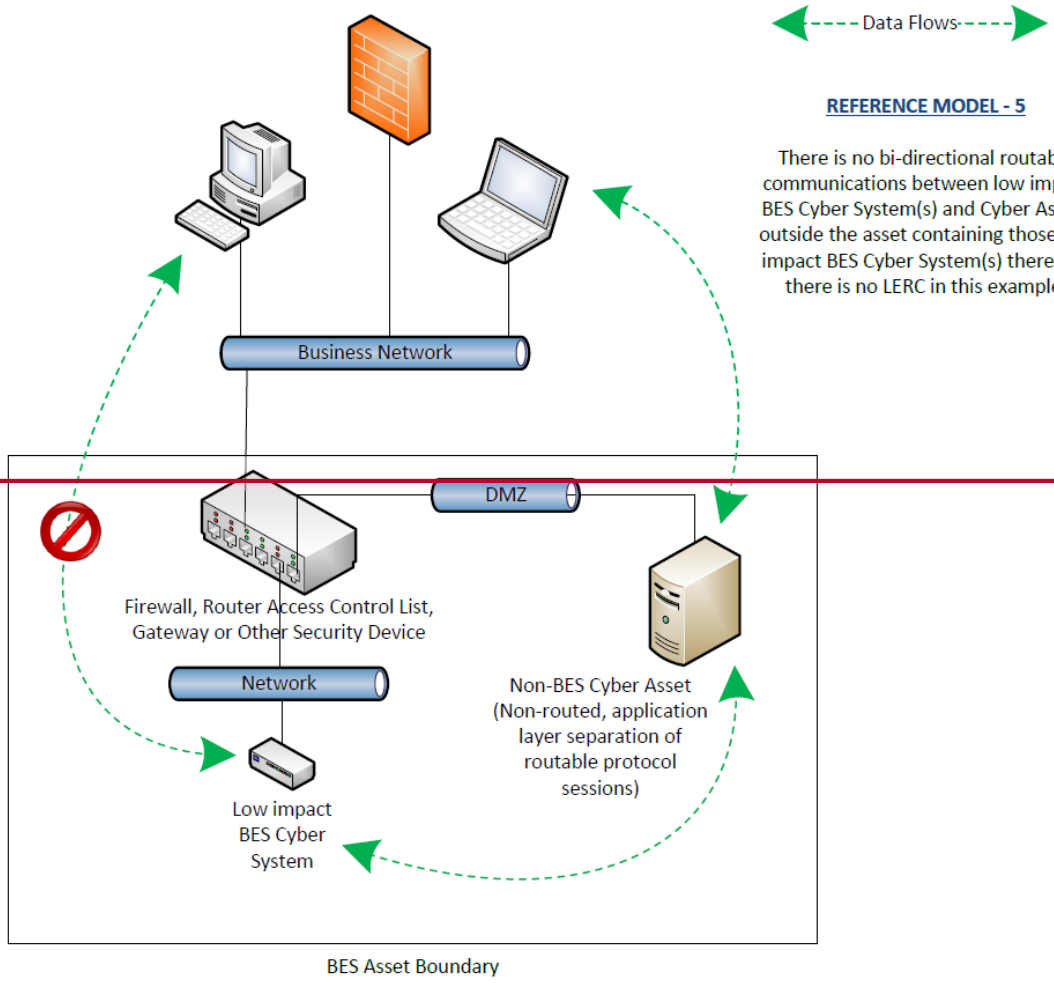

Data Flows
REFERENCE MODEL - 3
The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is place at "Location X" to act as the LEAP(s) and permit only necessary electronic access to the low impact BES Cyber Systems.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Location X
LERC
Network
Non BES Cyber Systsem
Low impact BES Cyber System
BES Asset Boundary
LERC
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

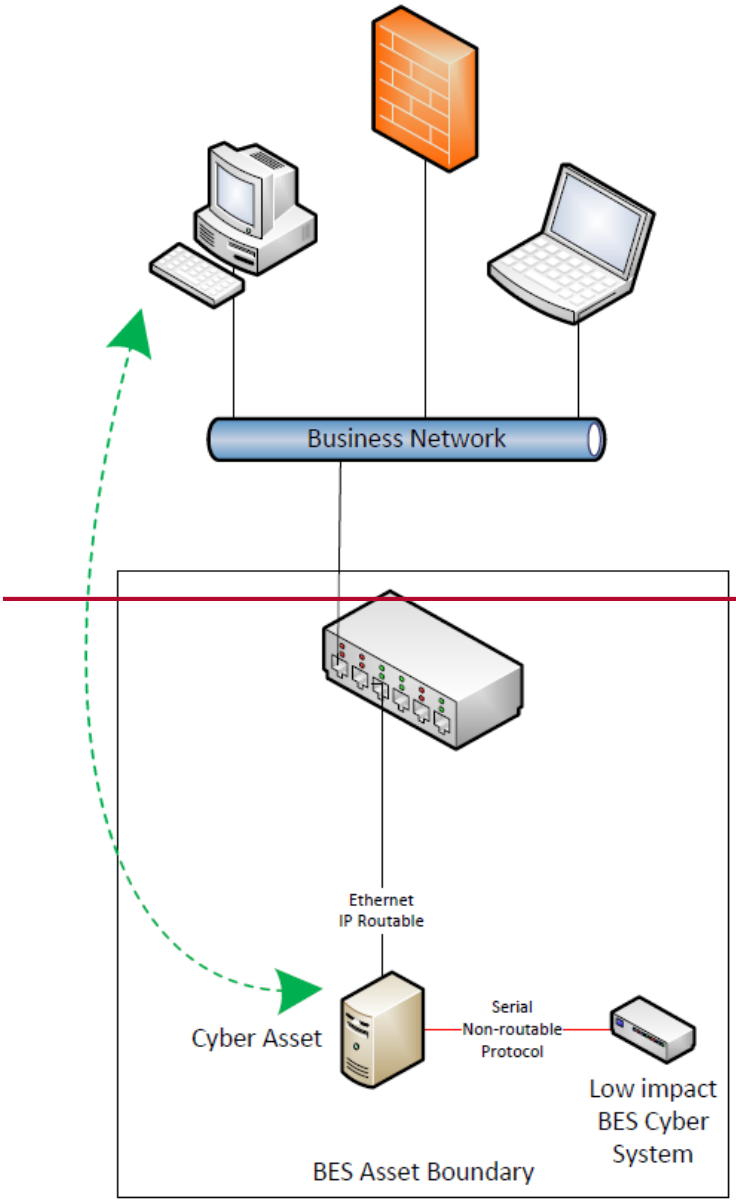


Data Flows

REFERENCE MODEL - 4

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.

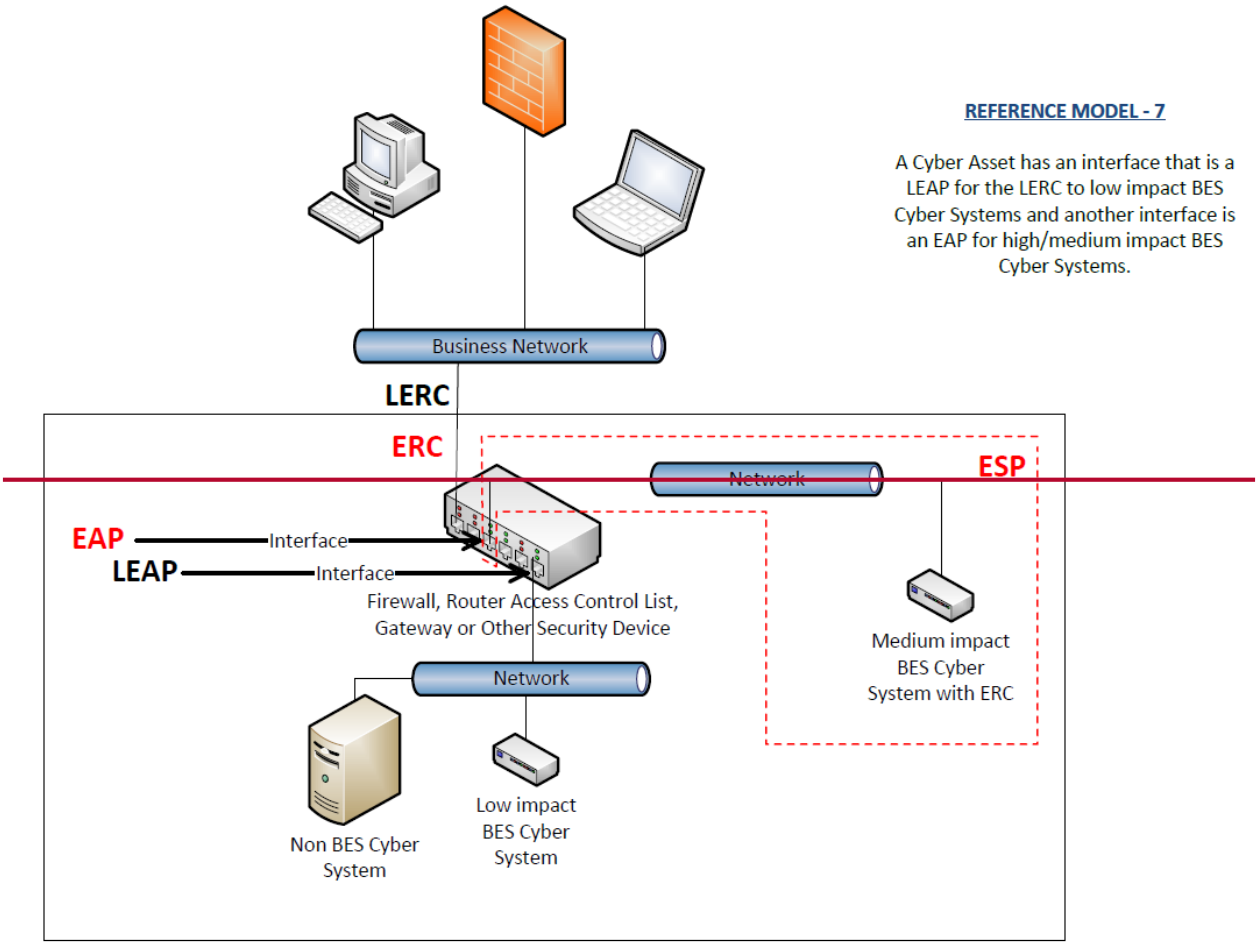

Data Flows
REFERENCE MODEL - 5
There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.
Business Network
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset (Non-routed, application layer separation of routable protocol sessions)
Low impact BES Cyber System
BES Asset Boundary



Data Flows

REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.



Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident

response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Responsible Entiteis need Transient Cyber Assets and Removable Media to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices, including specially-designed devices for maintaining equipment in support of the BES or a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Vulnerability Mitigation

The terms "mitigate", "mitigating", and "mitigation" are used in the sections in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation in this context does not necessarily require that each vulnerability be individually addressed or remediated, as many vulnerabilities may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is intended to mean that entities take steps to reduce security risks presented by connecting the Transient Cyber Asset or Removable Media.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset. When addressing malicious code protection, Section 5.1 obligates the Responsible Entities to implement methods to mitigate the introduction of malicious code on Transient Cyber Assets managed by the Responsible Entity.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that

maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is some additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- If a Responsible Entity chooses touse methods that mitigate the introduction of malicious code other than those listed, it should documentat how the other method(s) meet the mitigation of the introduction of malicious code objective.

If malicious code is discovered, it must be mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect toTransiet Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. is the SDT does not intend for the Responsible Entity to conduct a review for every single connection of that

Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is also not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party's and entity's actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This measure helps to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. However, the SDT does not intend for a Responsible Entity to conduct a review for every single connection of that Removable Media, but implement their process(es) in manner that protects all BES Cyber Systems where the Removable Media may be used. The intent is also not to require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-~~6~~7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-~~6~~7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented

authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System~~.~~(s). The cyber security plan(s) covers ~~four~~five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; ~~and~~ (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System~~.~~(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives

the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

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.

Description of Current Draft

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions to be incorporated into the Glossary of Terms Used in NERC Reliability Standards. In addition to approving the seven CIP Reliability Standards, the Commission, directed NERC to, among other things,: (1) "…develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems…", and (2) modify the definition of LERC.

In response to these directives, NERC first modified Reliability Standard CIP-003-6 to address the LERC directive, which has a regulatory deadline of March 31, 2017 for filing with the Commission. The revisions associated with the LERC directive were developed and posted for comment and ballot in July 2016 in draft Reliability Standard CIP-003-7. The revisions were not approved by stakeholders and based on the feedback received, the drafting team revised its approach and posted the revisions for an additional comment period and ballot. CIP-003-7 passed the additional ballot that ended on December 5, 2016.

For the transient device directive, NERC initially posted draft revisions for an informal comment period from November 1-18, 2016. This draft of Reliability Standard CIP-003-7(i) incorporates the proposed TCA language, as modified based on stakeholder comment, with the recently passed LERC revisions. The intent of this approach is to allow entities time to efficiently plan and implement the required modifications for low impact BES Cyber Systems. The Standard Drafting Team (SDT) approach to address the transient device directive is summarized below.

The SDT revised Attachment 1 of CIP-003-7 to include requirements that mitigate the risk to the BES of malware propagation from transient devices to low impact BES Cyber Systems. Attachment 1 contains and outlines the required sections of a Responsible Entity's cyber security plan(s) for its low impact BES Cyber Systems per Requirement R2. Previously, cyber security plan(s) were required to address four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. In keeping with the stakeholder approved approach to incorporate into one standard all the requirements applicable to assets containing low impact BES Cyber Systems, the SDT expanded CIP-003-7 Attachment 1 to include a fifth area: "Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation." Requiring the Responsible Entity to develop and implement these plans will provide higher assurance against the propagation of malware from transient devices.

In addition, the SDT determined it was necessary to revise the definitions of a Transient Cyber Asset (TCA) and Removable Media to ensure applicability of security controls and provide additional clarity. As well, the revised definitions accommodate use of the terms for all impact

levels: high, medium, and low. This is important for those entities that may opt to deploy one program to manage TCAs and Removable Media across multiple impact level assets.

The proposed revised definition of a Transient Cyber Asset (TCA) is:

A Cyber Asset that is:

1. *capable of transmitting or transferring executable code,*
2. *not included in a BES Cyber System,*
3. *not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and*
4. *directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:*
   - *BES Cyber Asset,*
   - *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
   - *PCA associated with high or medium impact BES Cyber Systems.*

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

The proposed revised definition of Removable Media is:

Storage media that:

1. *are not Cyber Assets,*
2. *are capable of transferring executable code,*
3. *can be used to store, copy, move, or access data, and*
4. *are directly connected for 30 consecutive calendar days or less to a:*
   - *BES Cyber Asset,*
   - *network within an Electronic Service Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
   - *Protected Cyber Asset associated with high or medium impact BES Cyber Systems.*

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

As proposed, Section 5 of Attachment 1 of CIP-003-7(i) mandates that entities have malware protection on TCAs (both entity and vendor-managed) and for Removable Media. The SDT proposes that it is necessary to distinguish between the specific protections for: (i) TCAs managed by the Responsible Entity, (ii) TCAs managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media.

For TCAs managed by the Responsible Entity, Section 5 requires the Responsible Entity to use one or a combination of the following to mitigate the introduction of malicious code: antivirus software, application whitelisting, or some other method. The SDT recognizes that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices (i.e., manage in an ongoing manner) while others have a checklist for transient devices prior to connecting them to a BES Cyber System (i.e., manage in an on-demand manner). The SDT acknowledges that both methods are effective and Section 5 permits either form of management. Because of the higher frequency in which these entity-managed devices are used, the controls required for these devices are more specific.

For Transient Cyber Assets managed by a party other than the Responsible Entity, Section 5 requires the Responsible Entity to review and verify the malware mitigation mechanism(s) used by the third party prior to connecting the Transient Cyber Asset (per Transient Cyber Asset capability).

For Removable Media, Section 5 requires entities to employ methods to detect malicious code and mitigate the threat of detected malicious code prior to connecting to a low impact BES Cyber System.

In summary, the SDT made the following changes to address the directive:

1. Revised the definitions of Transient Cyber Asset (TCA) and Removable Media.
2. Revised Requirement R1, by adding Parts 1.2.5 and 1.2.6 to include the complementary policies for the Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation in Requirement R2 (Attachment 1 of CIP-003-7(i)).
3. Revised the requirement language (Requirement R2) in Attachment 1 of CIP-003-7 by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation.
4. Revised the associated VSLs for Requirements R1 and R2 of CIP-003-7.
5. Revised the evidential language of Attachment 2 of CIP-003-7 by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to complement the revised requirement language.

Completed Actions	Date
Standard Authorization Request approved	July 20, 2016
Draft 1 of CIP-003-7(i) posted for formal comment and initial ballot	December 9, 2016 – January 23, 2017

Anticipated Actions	Date
10-day final ballot	February, 2017
NERC Board of Trustees adoption	February, 2017
Petition filed with FERC	March, 2017

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-7(i)

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. 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 SPS or RAS where the SPS or 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-003-7(i):

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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3. 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.

4.2.3.4. 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-003-7(i).

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls; ~~and~~

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation;

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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)(i)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)(i)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)(i)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the ~~four~~six topics required by R1. (R1.2) 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 BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the ~~four~~six topics required by R1. (R1.2) 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 BES Cyber Systems as	BES Cyber Systems, but did not address three of the ~~four~~six topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address ~~any~~four or more of the ~~four~~six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)(i)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	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. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	Systems as required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)(i)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)(i)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s)	containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented	failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)(i)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2)	its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification,	The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)(i)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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	according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)(i)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented	Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)(i)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				its plan(s) for Transient Cyber Assets and Removable Media, but 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 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)(i)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				to Requirement R2, Attachment 1, Section 5.3. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7)(i)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			delegated, but 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. (R4)	delegated, but 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. (R4)	changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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.	

Version	Date	Action	Change Tracking
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

Version	Date	Action	Change Tracking
			addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7(i)	TBD	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 ~~directive~~directives regarding (1) the definition of LERC and (2) transient devices.

Attachment 1

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

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

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

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

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The

focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

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

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

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

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security

Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Rationale for Section 5 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

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

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

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

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, the use of one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;

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

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

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

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

Attachment 2

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

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

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

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

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

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

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

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

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

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity;

evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability

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.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the ~~four~~six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a

combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such

communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located

at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

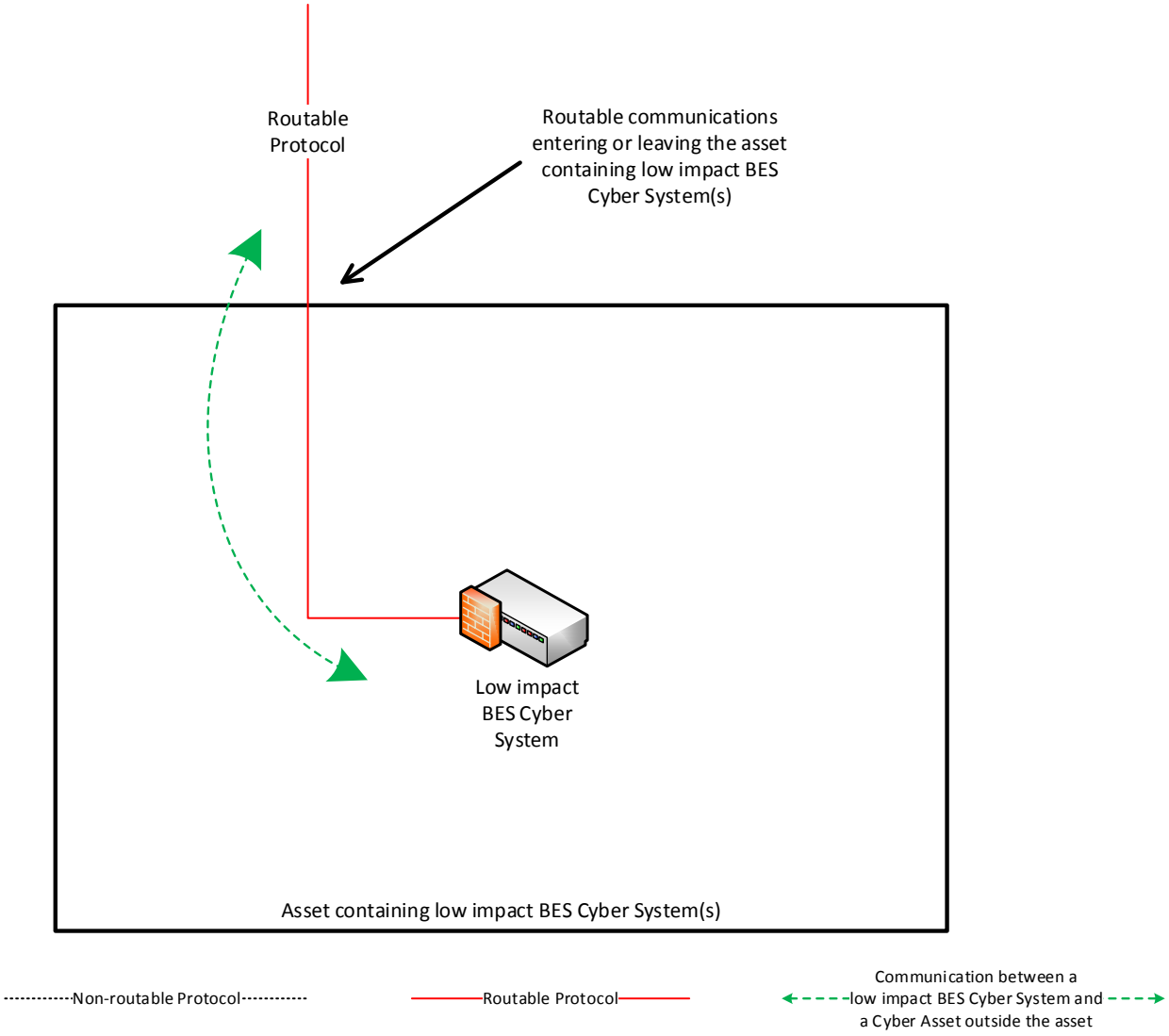
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

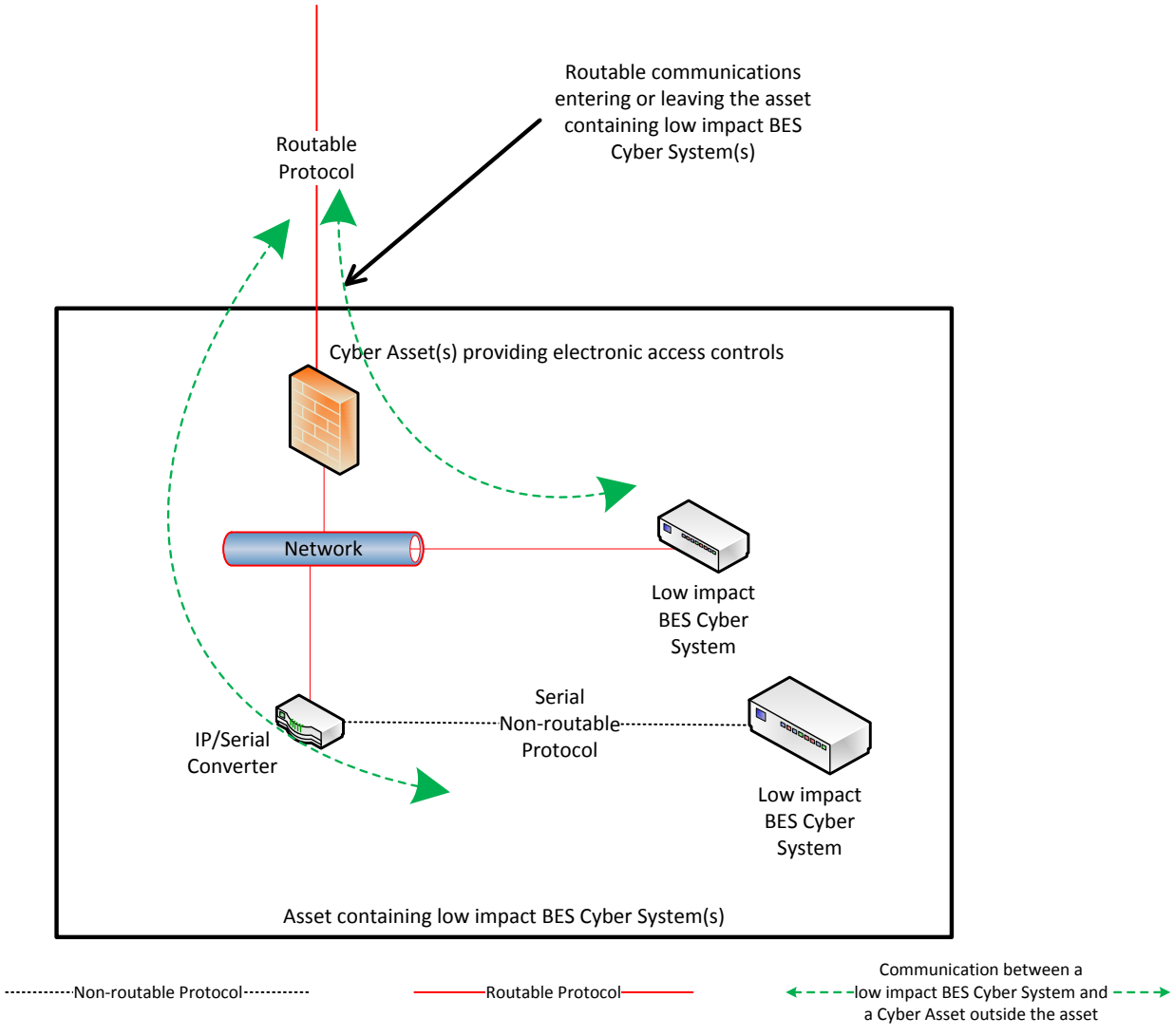
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

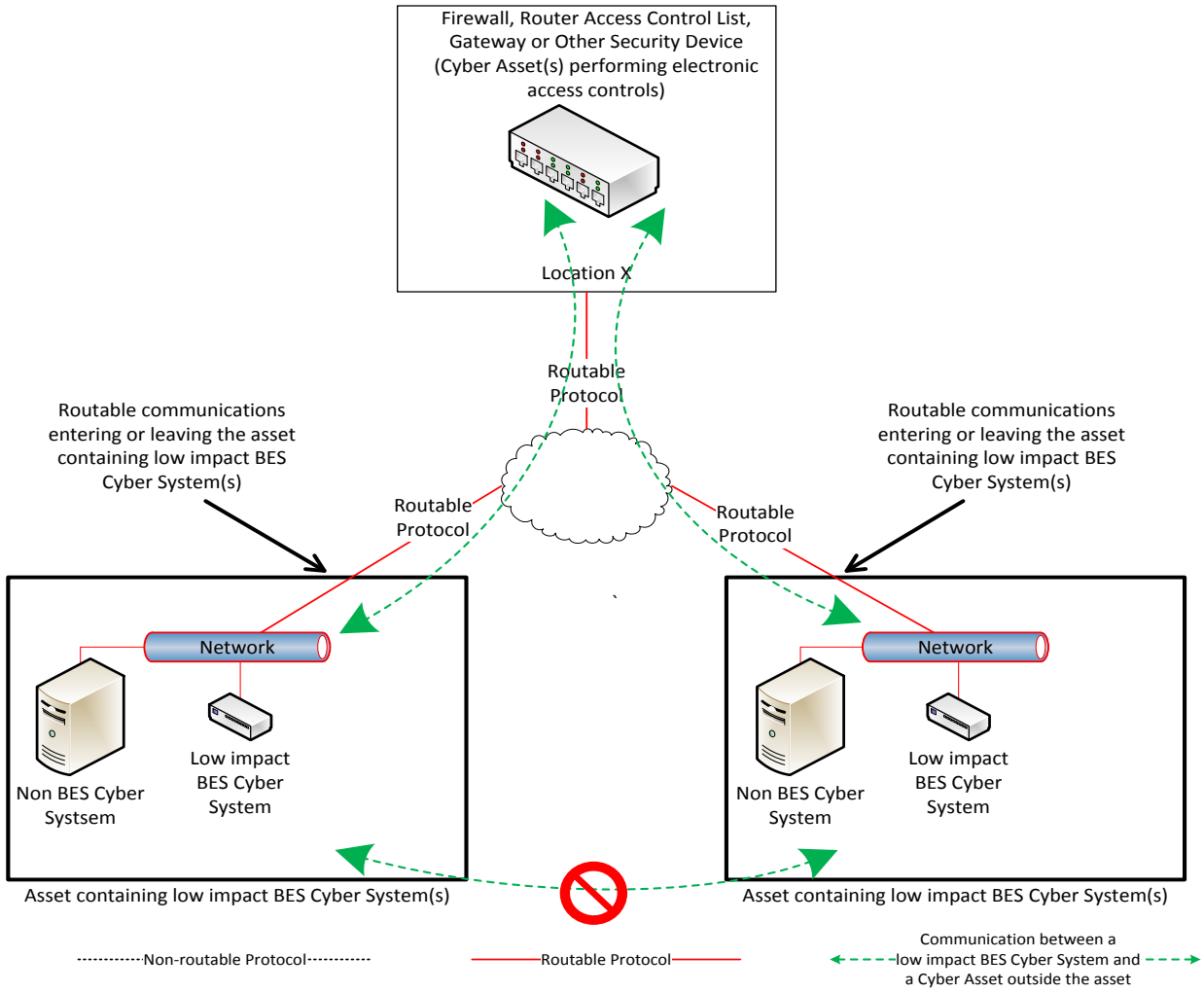
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

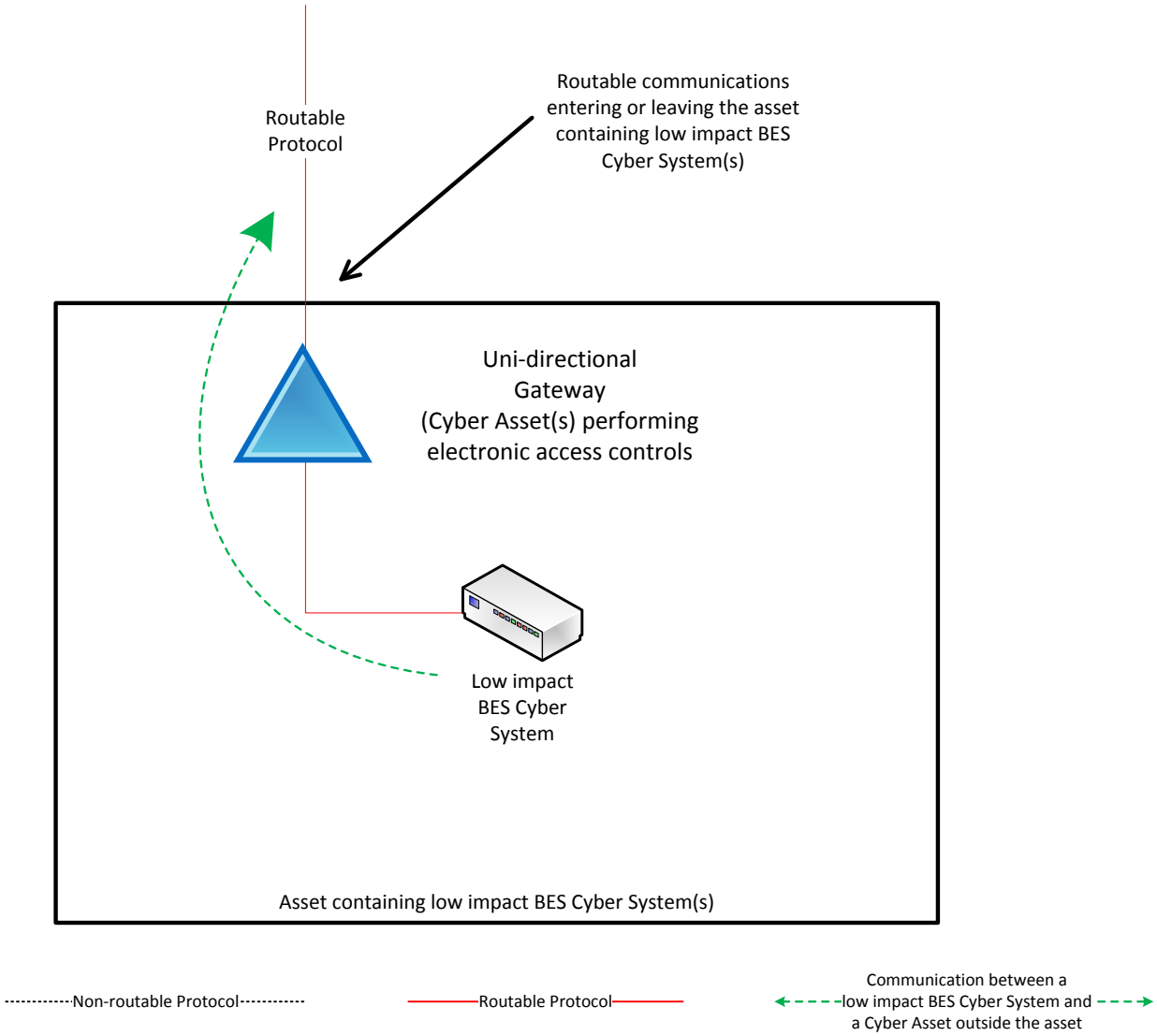
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

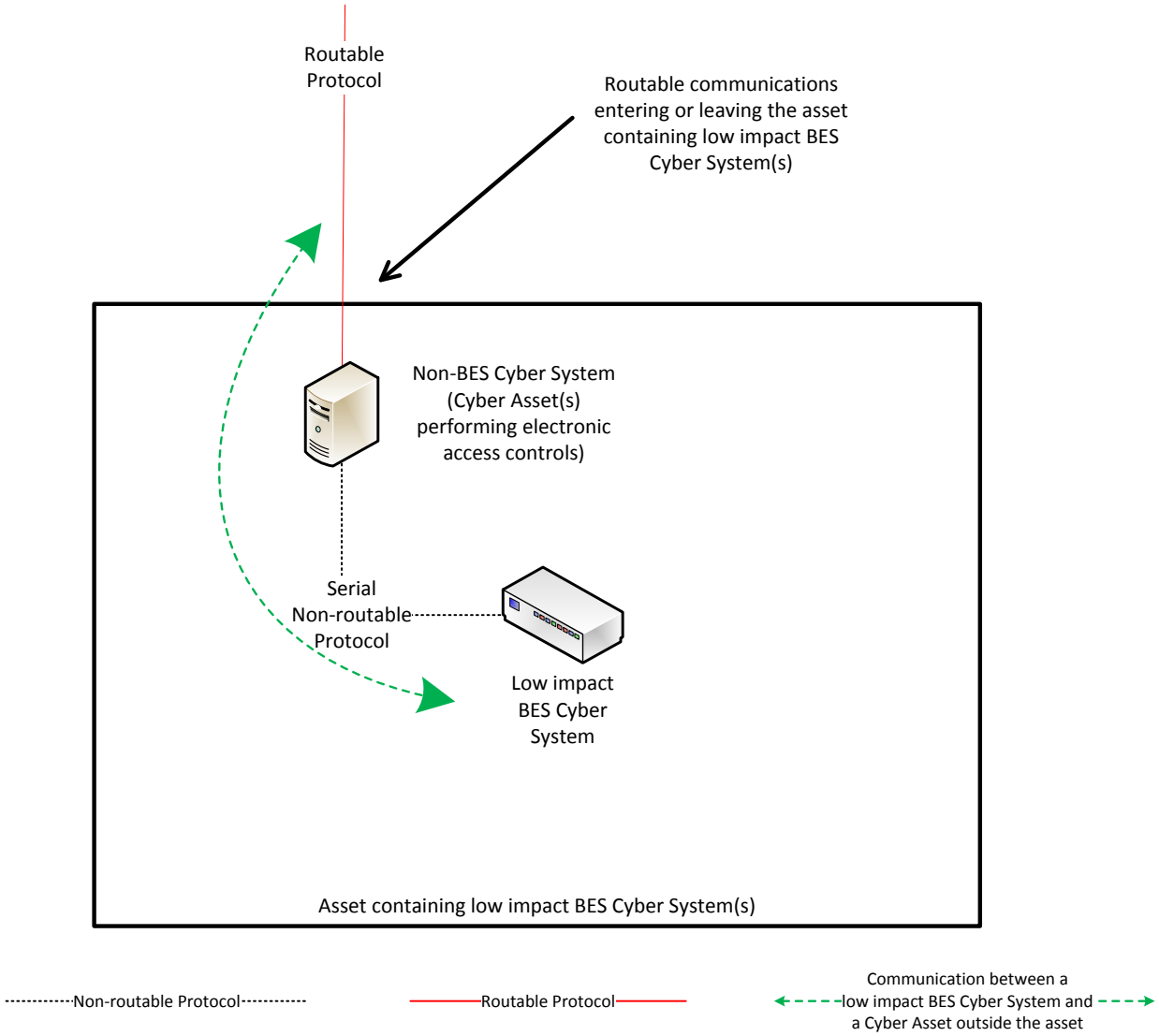
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

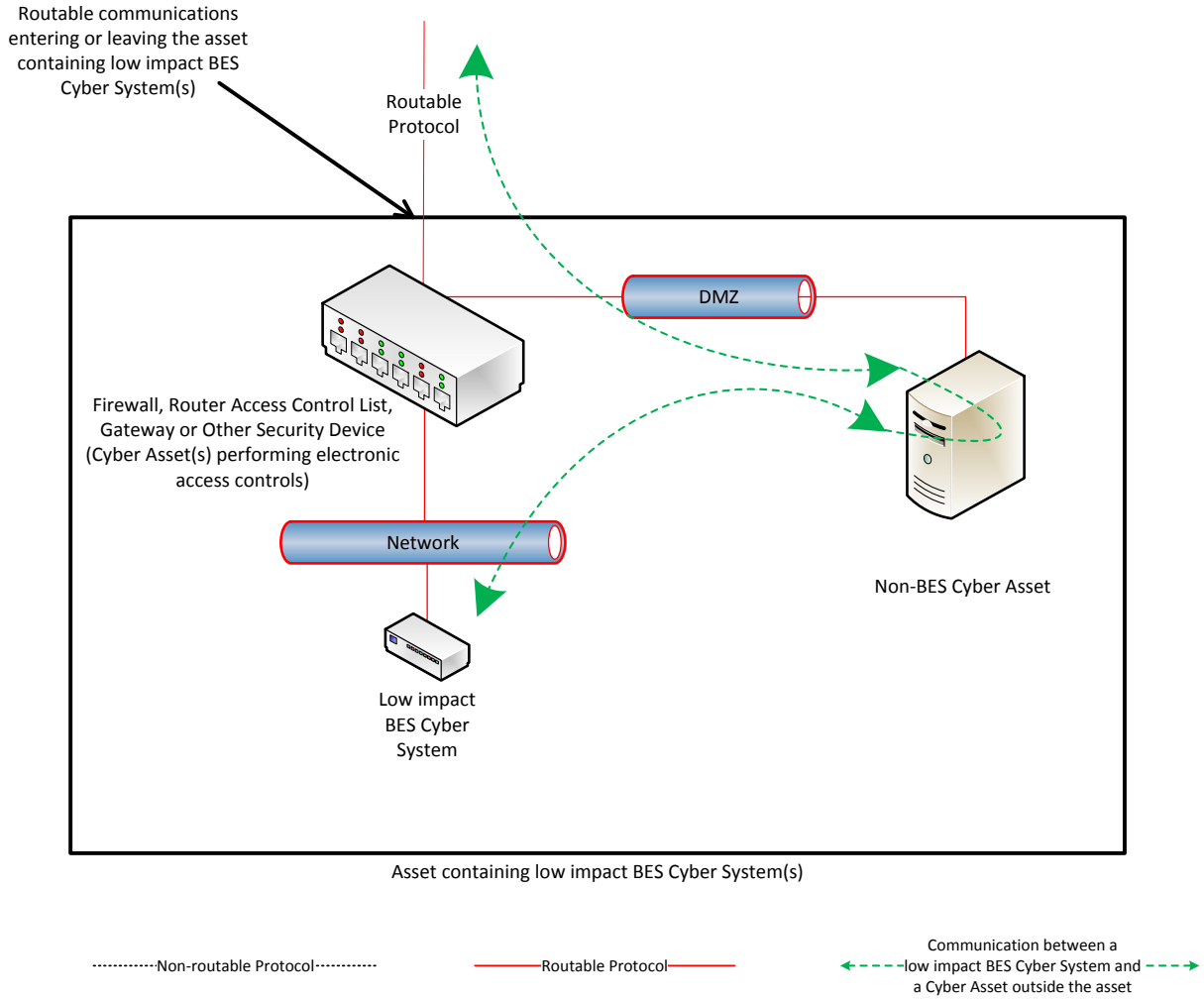
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

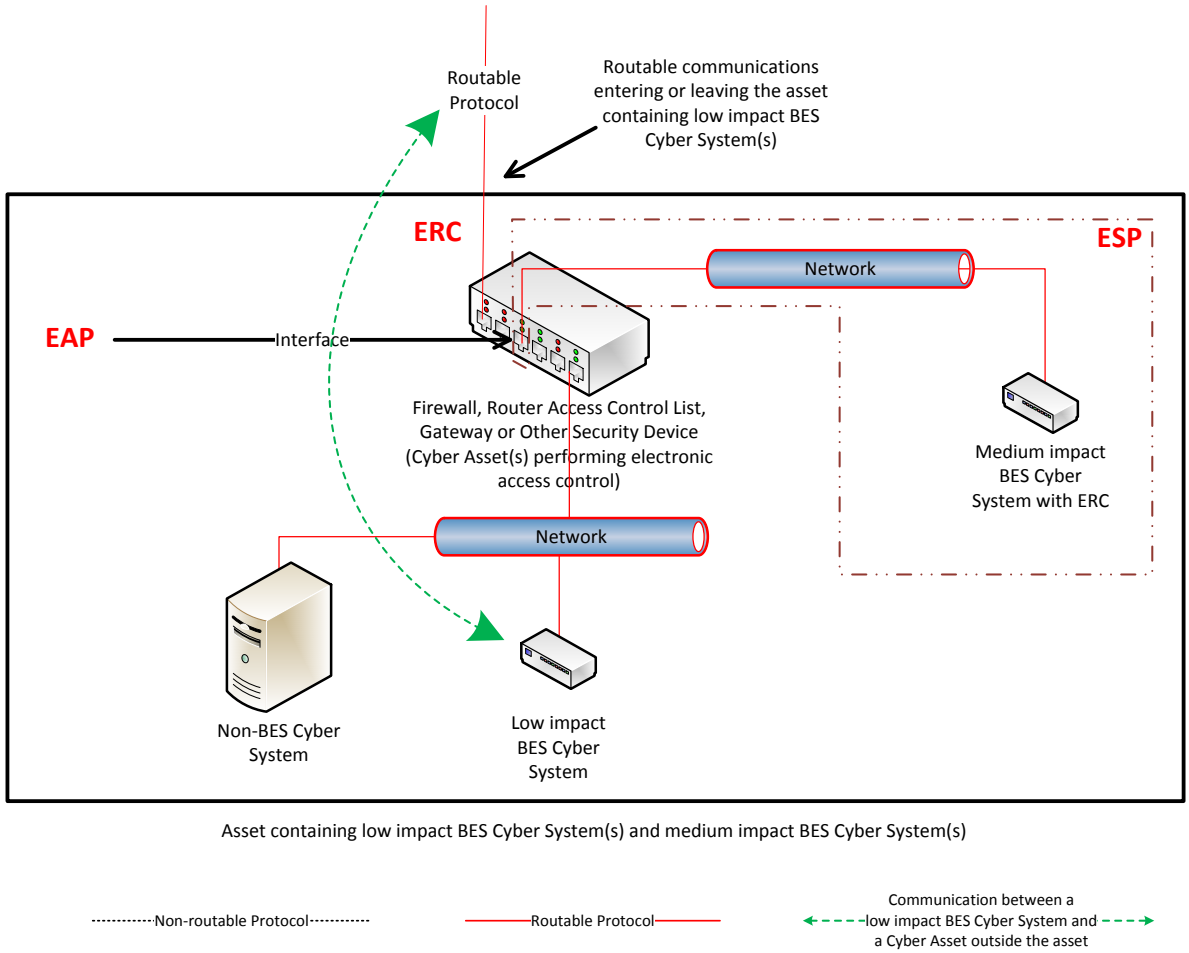
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.



Reference Model 7

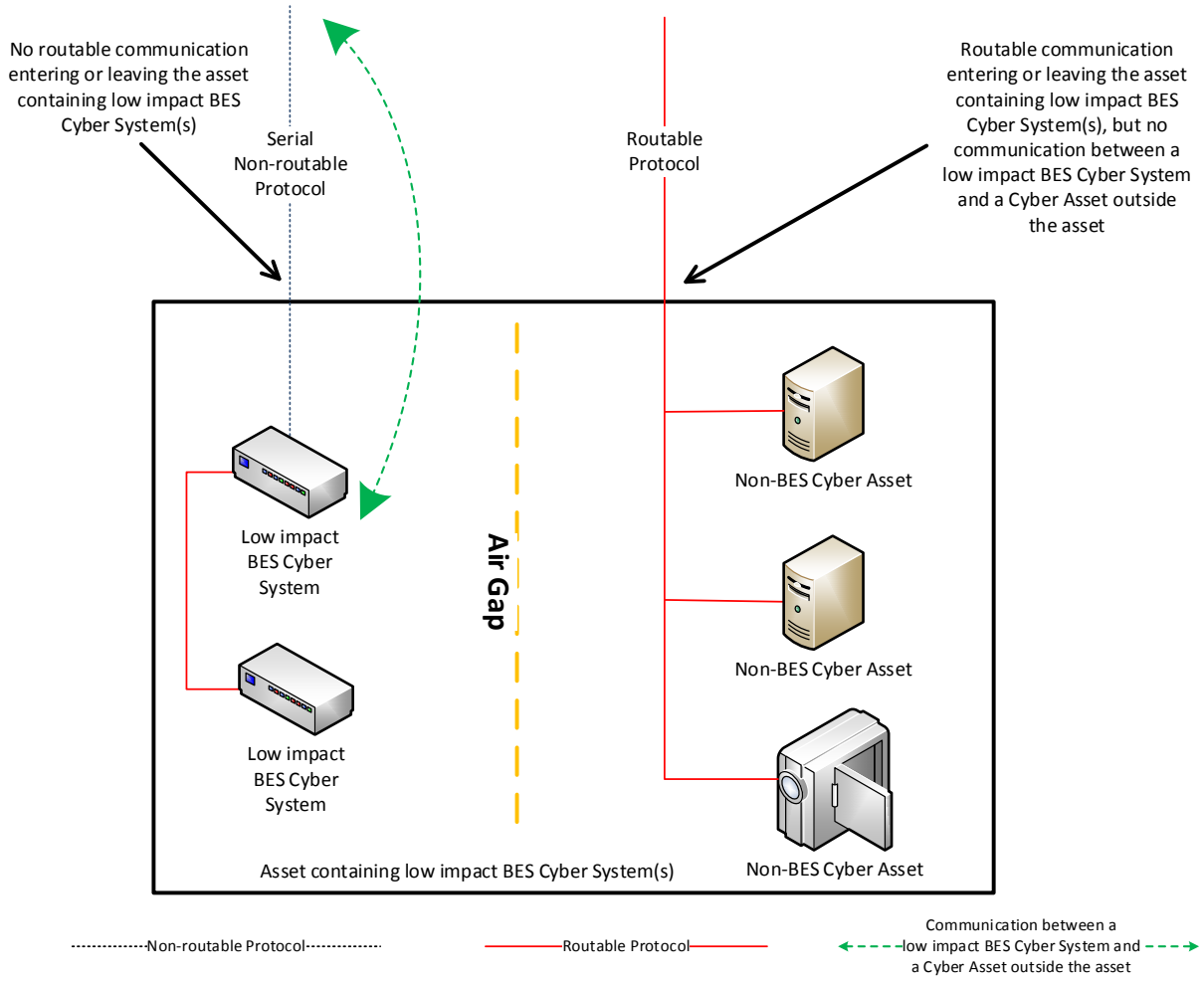
Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;

2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.

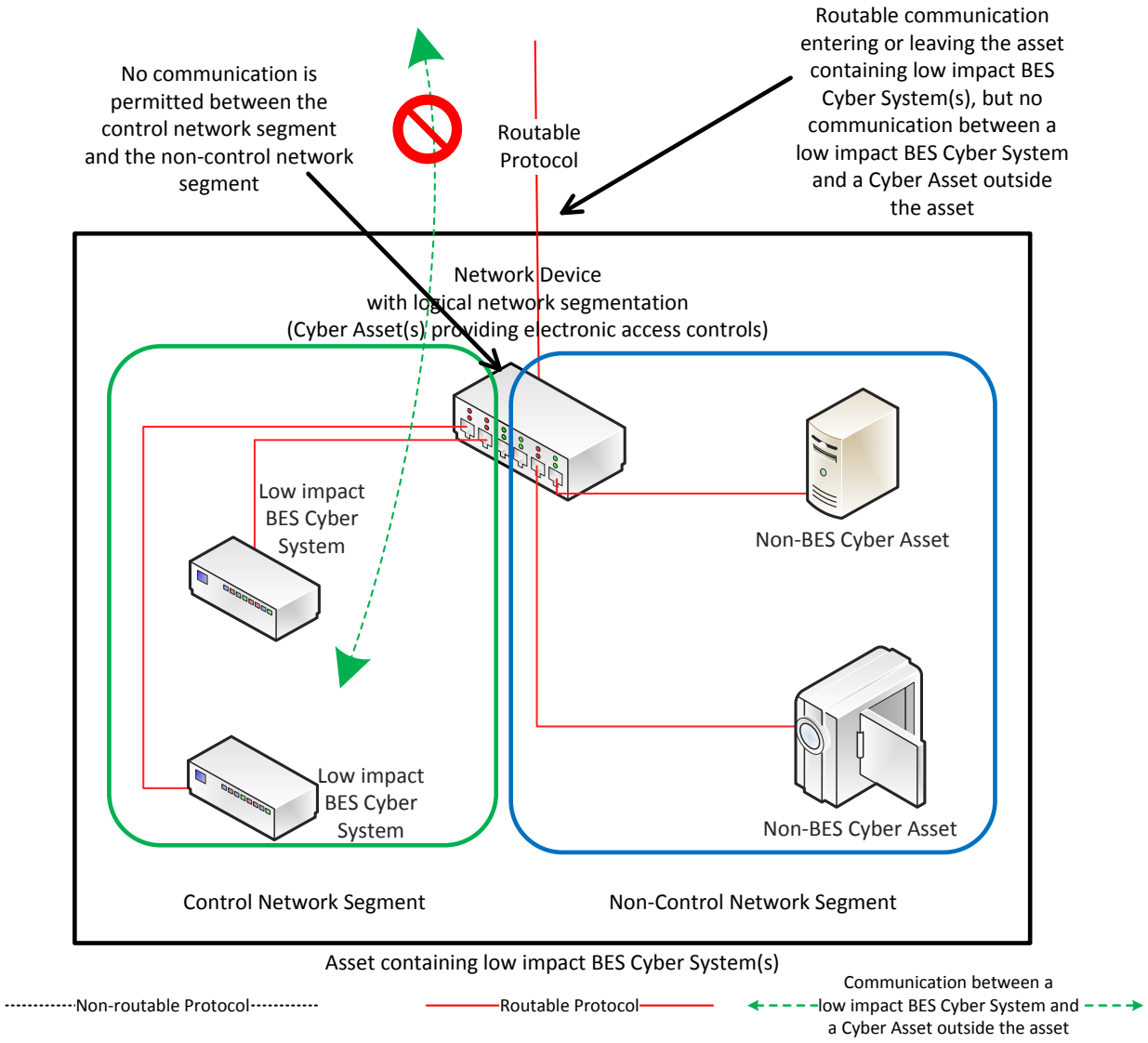
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

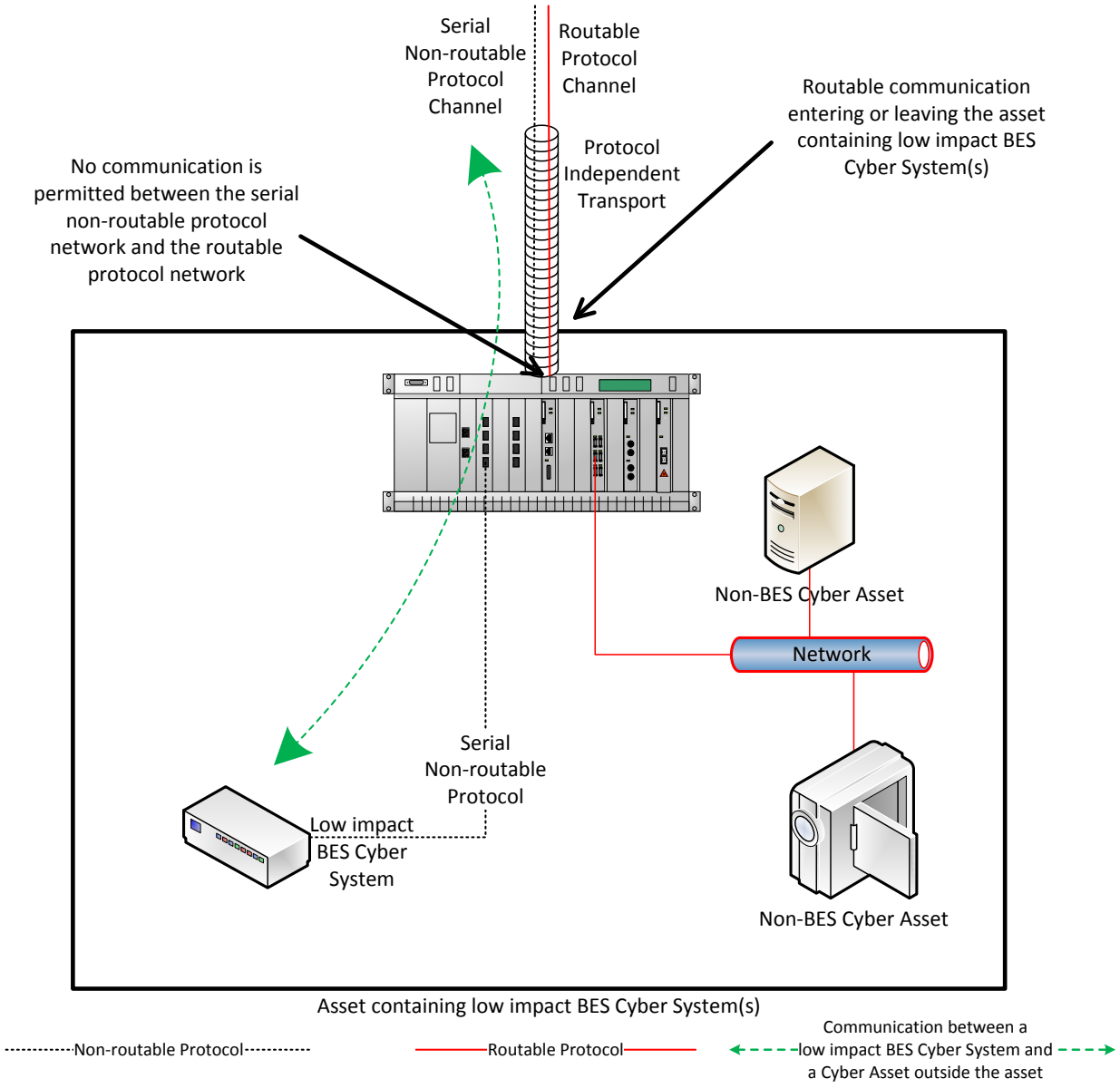
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Responsible Entiteis need Transient Cyber Assets and Removable Media to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices, including specially-designed devices for maintaining equipment in support of the BES or a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Vulnerability Mitigation

The terms "mitigate", "mitigating", and "mitigation" are used in the sections in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation in this context does not necessarily require that each vulnerability be individually addressed or remediated, as many vulnerabilities may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is intended to mean that entities take steps to reduce security risks presented by connecting the Transient Cyber Asset or Removable Media.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset. When addressing malicious code protection, Section 5.1 obligates the Responsible Entities to implement methods to mitigate the introduction of malicious code on Transient Cyber Assets managed by the Responsible Entity.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that

maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is some additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- If a Responsible Entity chooses touse methods that mitigate the introduction of malicious code other than those listed, it should documentat how the other method(s) meet the mitigation of the introduction of malicious code objective.

If malicious code is discovered, it must be mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect toTransiet Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. is the SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is

meeting the security objective. The intent is also not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party's and entity's actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This measure helps to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. However, the SDT does not intend for a Responsible Entity to conduct a review for every single connection of that Removable Media, but implement their process(es) in manner that protects all BES Cyber Systems where the Removable Media may be used. The intent is also not to require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated

the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers ~~four~~five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; ~~and~~ (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives

the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-003-7 - Cyber Security – Security Management Controls

Requested Approvals

- Reliability Standard CIP-003-7(i) - Cyber Security – Security Management Controls
- Definition of Transient Cyber Asset (TCA)
- Definition of Removable Media

Requested Retirements

- Reliability Standard CIP-003-6 - Cyber Security – Security Management Control
- Definition Low Impact BES Cyber System Electronic Access Point (LEAP)
- Definition of Low Impact External Routable Connectivity (LERC)
- Definition of Transient Cyber Asset (TCA)
- Definition of Removable Media

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions to be incorporated into the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary). In addition to approving the seven CIP Reliability Standards, the Commission, among other things, directed NERC to: (1) "develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems"; and (2) modify the definition of LERC in the NERC Glossary.

With respect to the transient devices directive, the Commission stated:

> 32. After consideration of the comments received on this issue, we conclude that the adoption of controls for transient devices used at Low Impact BES Cyber Systems, including Low Impact Control Centers, will provide an important enhancement to the security posture of the bulk electric system by reinforcing the defense-in-depth nature of the CIP Reliability Standards at all impact levels. Accordingly, we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.

For the LERC directive, the Commission stated:

> 73. Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

To address these directives, NERC modified Reliability Standard CIP-003. In responding to the transient devices directive, NERC modified the definitions of TCA and Removable Media. The revised definitions ensure the applicability of security controls, provide clarity, and accommodate the use of the terms for all impact levels: high, medium and low. The revised definitions will allow entities to deploy one program to manage TCAs and Removable Media across multiple impact levels.

Further, as an alternative to modifying the LERC definition, the standard drafting team retired the terms "LERC" and "LEAP", incorporating those concepts within the requirement language.

General Considerations

This Implementation Plan does not modify the effective date for CIP-003-6 in the Implementation Plan associated with CIP-003-6 nor any of the phased-in compliance dates included therein except that the compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7(i), provided in this Implementation Plan.

Further, this Implementation Plan clarifies that under Requirement R2 of CIP-003-7(i), the Responsible Entity shall not be required to include in its cyber security plan(s) any elements related to Sections 2, 3, and 5 of Attachment 1 until the effective date of CIP-003-7(i). Upon the effective date of CIP-003-7(i), the Responsible Entity's cyber security plan(s) must include the elements required by Sections 2, 3, and 5 of Attachment 1 and the Responsible Entity must implement the controls included in its plan to meet the objectives of Sections 2, 3, and 5.

Effective Dates

The effective dates for the proposed Reliability Standard and NERC Glossary terms are provided below.

Reliability Standard CIP-003-7(i)

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7(i) shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-7(i) shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

NERC Glossary Definitions of Transient Cyber Asset and Removable Media

Where approval by an applicable governmental authority is required, the definitions of Transient Cyber Asset and Removable Media shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the definitions, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the definitions of Transient Cyber Asset and Removable Media shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the date that the definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Planned or Unplanned Changes

Planned or Unplanned Changes Resulting in a Higher Categorization – This Implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-5 titled Planned or Unplanned Changes Resulting in a Higher Categorization.[1]

Unplanned Changes Resulting in Low Impact Categorization – This Implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-6 titled Unplanned Changes Resulting in Low Impact Categorization. That section provides:

> For unplanned changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

Retirement Date

Reliability Standard CIP-003-6

Reliability Standard CIP-003-6 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-7(i) in the particular jurisdiction in which the revised standard is becoming effective.

Current NERC Glossary of Terms Definition(s) of LERC, LEAP, TCA and Removable Media

The current definitions of LERC and LEAP shall be retired from the NERC Glossary immediately prior to the effective date of Reliability Standard CIP-003-7(i) in the particular jurisdiction in which the revised standard is becoming effective.

The current definitions of Transient Cyber Asset and Removable Media shall be retired from the NERC Glossary immediately prior to the effective date of the revised definitions for those terms in the particular jurisdiction in which the revised definitions are becoming effective.

[1] Due to the length of that section, it is not reproduced herein.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed Definitions of: "Transient Cyber Asset" (TCA) and "Removable Media"

Term: "Transient Cyber Asset" (TCA)

Revised Definition:

A Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Redline Definition:

A Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Currently Approved Definition of "Transient Cyber Asset" (TCA):

A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Term: "Removable Media"

Revised Definition:

Storage media that:

1. are not Cyber Assets,
2. are capable of transferring executable code,
3. can be used to store, copy, move, or access data, and
4. are directly connected for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Redline Definition:

Storage media that:

1. are not Cyber Assets,
2. are capable of transferring executable code,
3. can be used to store, copy, move, or access data, and
4. are directly connected for 30 consecutive calendar days or less to a:
   - BES Cyber Asset, ~~a~~
   - network within an Electronic Security Perimeter (ESP)~~,~~ containing high or medium impact BES Cyber Systems, or ~~a~~
   - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Currently Approved Definition of "Transient Cyber Asset" (TCA):

Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Requirements for Transient Cyber Assets – CIP-003-7(i)

Do not use this form for submitting comments. Use the electronic form to submit comments on the **Modifications to address the Federal Energy Regulatory Commission (FERC or the Commission) directive regarding the mandatory protection for transient devices used at Low Impact BES Cyber Systems.** The electronic form must be submitted by **8 p.m. Eastern, Wednesday, January 25, 2017.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Al McMeekin at (404) 446-9675.

Description of Current Draft

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions to be incorporated into the Glossary of Terms Used in NERC Reliability Standards. In addition to approving the seven CIP Reliability Standards, the Commission, directed NERC to, among other things,: (1) "…develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems…", and (2) modify the definition of LERC. On March 9, 2016, the NERC Standards Committee authorized the Standards Authorization Request (SAR) to be posted for a 30-day informal comment period from March 23 – April 21, 2016. Based on the comments received, the 2016-02 Modifications to CIP Standards Drafting Team (SDT) made minor revisions to the SAR which was posted for an additional 30-day informal comment period June 1-30, 2016.

In Order 822, the Commission stated:

> 32. After consideration of the comments received on this issue, we conclude that the adoption of controls for transient devices used at Low Impact BES Cyber Systems, including Low Impact Control Centers, will provide an important enhancement to the security posture of the bulk electric system by reinforcing the defense-in-depth nature of the CIP Reliability Standards at all impact levels. Accordingly, we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.

The SDT revised Attachment 1 of CIP-003-7 to require the mitigation of risk to the BES of malware propagation from transient devices to low impact BES Cyber Systems. Attachment 1 contains and outlines

the required sections of a Responsible Entity's cyber security plan(s) for its low impact BES Cyber Systems per Requirement R2. Previously, cyber security plan(s) were required to address four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. In keeping with the stakeholder approved approach to incorporate into one standard all the requirements applicable to assets containing low impact BES Cyber Systems, the SDT expanded CIP-003-7 Attachment 1 to include a fifth area: "Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation." Requiring the Responsible Entity to develop and implement these plans will provide mitigation for malware propagation to BES Cyber Systems from transient devices.
In addition, the SDT determined it was necessary to revise the definitions of a Transient Cyber Asset (TCA) and Removable Media to ensure applicability of security controls and provide additional clarity. As well, the revised definitions accommodate use of the terms for all impact levels: high, medium and low. This is important for those entities that may opt to deploy one program to manage TCAs and Removable Media across multiple impact level assets.

The proposed definition of a Transient Cyber Asset (TCA) is:

A Cyber Asset that is:

1. *capable of transmitting or transferring executable code,*
2. *not included in a BES Cyber System,*
3. *not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and*
4. *directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:*
   - *BES Cyber Asset,*
   - *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
   - *PCA associated with high or medium impact BES Cyber Systems.*

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

The proposed definition of Removable Media is:

Storage media that:

1. *are not Cyber Assets,*
2. *are capable of transferring executable code,*
3. *can be used to store, copy, move, or access data, and*
4. *are directly connected for 30 consecutive calendar days or less to a:*
   - *BES Cyber Asset,*
   - *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
   - *Protected Cyber Asset associated with high or medium impact BES Cyber Systems.*

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

As proposed, Section 5 of Attachment 1 of CIP-003-7(i) mandates that entities have malware protection for Transient Cyber Assets (both entity and vendor-managed) and Removable Media. The SDT proposes that it is necessary to distinguish between the specific protections for: (i) Transient Cyber Assets managed by the Responsible Entity, (ii) Transient Cyber Assets managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media.

For Transient Cyber Assets managed by the Responsible Entity, Section 5 requires the Responsible Entity to use one or a combination of the following to mitigate the introduction of malicious code: antivirus software, application whitelisting, or some other method. The SDT recognized that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices (i.e., manage in an ongoing manner) while others have a checklist for transient devices prior to connecting them to a BES Cyber System (i.e., manage in an on-demand manner). The SDT acknowledges both methods are effective and Section 5 permits either form of management. Because of the higher frequency in which these entity-managed devices are used, the controls required for these devices are more specific.

For Transient Cyber Assets managed by a party other than the Responsible Entity, Section 5 requires the Responsible Entity to review and verify the malware mitigation mechanism(s) used by the third party prior to connecting the Transient Cyber Asset (per Transient Cyber Asset capability).

For Removable Media, Section 5 requires entities to employ method(s) to detect malicious code and mitigate the threat of detected malicious code prior to connecting to a low impact BES Cyber System.

In summary, the SDT made the following changes to address the directive:

1. Revised the definitions of Transient Cyber Asset and Removable Media.
2. Revised Requirement R1, by adding Parts 1.2.5 and 1.2.6 to include the complementary policies for the Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation in Requirement R2 (Attachment 1 of CIP-003-7(i)).
3. Revised the requirement language (Requirement R2) in Attachment 1 of CIP-003-7(i) by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation.
4. Revised the associated VSLs for Requirement R2 of CIP-003-7(i).
5. Revised the evidential language of Attachment 2 of CIP-003-7(i) by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to complement the revised requirement language.

Development Plan for LERC and TCA Modifications

The CIP Modifications Standard Drafting Team is currently addressing eight issue areas within the CIP standards including two FERC directed issue areas that directly impact the requirements for low impact BES Cyber Systems - the Low Impact External Routable Connectivity (LERC) modifications and requirements for TCAs used at assets containing low impact BES Cyber Systems. The LERC modifications

have a regulatory filing deadline of March 31, 2017. Through outreach, stakeholders have expressed a preference for the SDT to consolidate, as much as possible, proposed changes to the standards that pertain to assets containing low impact BES Cyber Systems and to do so expeditiously. The consolidation would foster stability in the low impact requirements and enable efficient implementation of the requirements which is important given the volume of in-scope assets and the work currently underway for CIP-003-6. Consequently, the SDT and NERC staff are exploring opportunities to accomplish this objective.

This posting combines the language from the successful ballot of CIP-003-7 (Low Impact External Routable Connectivity (LERC) modifications) and the language from the informal posting of CIP-003-TCA (transient devices at low impact modifications) along with revisions based on stakeholder feedback. A successful ballot of CIP-003-7(i) will permit the SDT to complete a final ballot of the combined LERC and TCA language prior to the FERC deadline for the LERC modifications of March 31, 2017.

The SDT is seeking feedback on the draft TCA requirements in CIP-003-7(i). The TCA proposal uses a subset of the language from the CIP-010 TCA requirements commensurate with the risk associated at low impact BES Cyber Systems. The CIP-003-7(i) language is consistent with the existing TCA language for Medium and High Impact BES Cyber Systems to enable a common understanding of the requirements, particularly for those entities implementing a plan to cover high, medium and low impact.

Receiving thoughtful and constructive feedback from stakeholders is critical to the success of this plan. Submitting comments in advance of the deadline is welcome. The SDT thanks you for your participation.

Questions

1. Definition: The SDT revised the definition of Transient Cyber Asset such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

2. Definition: The SDT revised the definition of Removable Media such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

3. Requirement R2: The SDT revised CIP-003-7(i), Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to mitigate the risk of propagation of

malware from transient devices. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Yes:

No:

Comments:

4. Attachment 2: The SDT revised the evidential language of CIP-003-7(i), Attachment 2, Section 5 to make the Measures consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes:

   No:

   Comments:

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides examples of temporarily connected devices, and strategies to consider in developing the Transient Cyber Asset and Removable Media malicious code mitigation plan(s) at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

   Yes:

   No:

   Comments:

6. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

   Yes:

   No:

   Comments:

7. If you have additional comments on the proposed revisions to address the FERC directive regarding TCAs for low impact BES Cyber Systems that you have **not** provided in response to the questions above, please provide them here.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of the violation risk factor (VRF) and violation severity levels (VSLs) for Requirements R1 and R2 in proposed NERC Reliability Standard CIP-003-7(i) - Cyber Security — Security Management Controls. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-003-7(i), Requirement R2	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Lower was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements for low impact BES Cyber Systems. The purpose of the plan is for entities to develop an approach involving multiple procedures to address a broad subject matter. Using a plan, Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems.
FERC VRF G1 Discussion Guideline 1 - Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2 - Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement a documented cyber security plan that contains certain sections specified in Attachment 1. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security plan, the VRF is reflective of the plan as a whole. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain low impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3 - Consistency among Reliability Standards	This requirement maps from CIP-003-6, Requirement R2, which has an approved VRF of Lower; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Failure to properly implement the cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state

VRF Justifications for CIP-003-7(i), Requirement R2	
Proposed VRF	**Lower**
Guideline 4 - Consistency with NERC Definitions of VRFs	or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion Guideline 5 - Treatment of Requirements that Co-mingle More than One Obligation	The cyber security plan requirement encompasses a number of subject matter areas for low impact BES Cyber Systems. The VRF is identified at the risk level represented by all of the plan areas in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.

VSLs for CIP-003-7(i), Requirement R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES

VSLs for CIP-003-7(i), Requirement R1			
Lower	**Moderate**	**High**	**Severe**
impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the six topics required by R1. (R1.2)	impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the six topics required by R1. (R1.2)	impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the six topics required by R1. (R1.2)	Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more

VSLs for CIP-003-7(i), Requirement R1			
Lower	**Moderate**	**High**	**Severe**
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 BES Cyber Systems 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. (R1.2) 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 BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems 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. (R1.2) 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 BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) 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 BES Cyber Systems 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. (R1.2)	of the six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

VSL Justifications for CIP-003-7(i), Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved Requirement R1, CIP-003-6. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-003-7(i), Requirement R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security policy(s) but fails to include one or more of the required sections of Attachment 1. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The action of the requirement is to document cyber security policy(s). Implementation of the cyber security policy(s) is demonstrated through performance of Requirement R2. There is no documentation and implementation interdependence within Requirement R1.

VSLs for CIP-003-7(i), Requirement R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented its cyber security	The Responsible Entity documented its cyber security	The Responsible Entity documented the physical access	The Responsible Entity failed to document and implement one

VSLs for CIP-003-7(i), Requirement R2			
Lower	**Moderate**	**High**	**Severe**
plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber	plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR	controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36	or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

VSLs for CIP-003-7(i), Requirement R2			
Lower	**Moderate**	**High**	**Severe**
Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing	calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR	

VSLs for CIP-003-7(i), Requirement R2			
Lower	**Moderate**	**High**	**Severe**
	low impact BES Cyber Systems, but failed to document the 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	

VSLs for CIP-003-7(i), Requirement R2			
Lower	**Moderate**	**High**	**Severe**
	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 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)		

VSL Justifications for CIP-003-7(i), Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved Requirement R2, CIP-003-6. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-003-7(i), Requirement R2	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security plan(s) but fails to address one or more of the required sections of Attachment 1. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The action of the requirement is to implement documented cyber security plan(s). Documentation of the plan(s) is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the plan in this case; as such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity implemented all the required elements of the plan. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2016-02 Modifications to CIP Standards

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
After consideration of the comments received on this issue, we conclude that the adoption of controls for transient devices used at Low Impact BES Cyber Systems, including Low Impact Control Centers, will provide an important enhancement to the security posture of the bulk electric system by reinforcing the defense-in-depth nature of the CIP Reliability Standards at all impact levels. Accordingly, we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.	FERC Order 822, Paragraph 32; issued January 21, 2016	The Project 2016-02 Standard Drafting Team (SDT) revised Attachment 1 of CIP-003-7(i) to mitigate the risk to the BES of malware propagation to low impact BES Cyber Systems from transient devices. Attachment 1 contains and outlines the required sections of a Responsible Entity's cyber security plan(s) for its low impact BES Cyber Systems per Requirement R2. Previously, cyber security plan(s) were required to address four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. In keeping with the stakeholder approved approach to incorporate all the requirements applicable to assets containing low impact BES Cyber Systems into one standard, the SDT expanded CIP-003-7 Attachment 1 to include a fifth area: "Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation". Requiring the Responsible Entity to develop and implement these plans will provide higher assurance against the propagation of malware from transient devices. The plan approach for TCAs and Removable Media is consistent with the existing requirement

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		structure applicable to lows and accommodates the risk level of the assets. Additionally, the SDT revised the definitions of Transient Cyber Asset (TCA) and Removable Media. The revised definitions ensure the applicability of security controls, provide clarity, and accommodate the use of the terms for all impact levels: high, medium and low. The revised definitions will allow entities to deploy one program to manage TCAs and Removable Media across multiple impact levels. The revised definition of a Transient Cyber Asset (TCA) is: A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		• PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. The revised definition of Removable Media is: Storage media that: 1. are not Cyber Assets, 2. are capable of transferring executable code, 3. can be used to store, copy, move, or access data, and 4. are directly connected for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Service Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • Protected Cyber Asset associated with high or medium impact BES Cyber Systems. Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		drives, and other flash memory cards/drives that contain nonvolatile memory. As proposed, Section 5 of Attachment 1 of CIP-003-7(i) mandates that entities have malware protection on Transient Cyber Assets (both entity and vendor-managed) and for Removable Media. The SDT determined that it was necessary to distinguish between the specific protections for: (i) Transient Cyber Assets managed by the Responsible Entity, (ii) Transient Cyber Assets managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media. For Transient Cyber Assets managed by the Responsible Entity, Section 5 requires Responsible Entities to use one or a combination of the following to mitigate the introduction of malicious code: antivirus software, application whitelisting, or some other method. The SDT recognizes that Responsible Entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices (i.e., manage in an ongoing manner) while others have a checklist for transient devices prior to connecting them to a BES Cyber System (i.e., manage in an on-demand manner). The drafting team acknowledges both methods are effective and Section 5 permits either form of management. Because of the higher

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		frequency in which these entity-managed devices are used, the controls required for these devices are more specific. For Transient Cyber Assets managed by a party other than the Responsible Entity, Section 5 requires the Responsible Entity to review and verify the malware mitigation mechanism(s) used by the third party prior to connecting the Transient Cyber Asset (per Transient Cyber Asset capability). For Removable Media, Section 5 requires entities to employ methods to detect malicious code and mitigate the threat of detected malicious code prior to connecting to a low impact BES Cyber System.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Reminder and Update
Project 2016-02 Modifications to CIP Standards

Initial Ballots and Non-binding Poll Open through January 25, 2017

Now Available

The following ballots are open through **8 p.m. Eastern, Wednesday, January 25, 2017**:

1. **CIP-003-7(i) - Cyber Security – Security Management Controls**
2. **CIP-003-7(i) Implementation Plan**
3. **Transient Cyber Asset (TCA) - Proposed revised definition**
4. **Removable Media - Proposed revised definition**
5. **CIP-003-7(i) Non-binding Poll**

Draft Reliability Standard Audit Worksheet (RSAW) Update

The draft RSAW for **CIP-003-7(i) - Cyber Security – Security Management Controls** (announced on January 4, 2017) that is currently posted on the **project page** is being revised to clarify a section related to auditor instructions. The revised RSAW will be posted, announced, and available for review during the week of January 16, 2017.

Balloting

Members of the ballot pools associated with this project may log in and submit their vote for the standard and its implementation plan, the new terms and their definition, and the non-binding poll by clicking here. If you experience any difficulties in using the electronic form, contact Wendy Muller.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*

*Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Al McMeekin at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards
CIP-003-7(i)

Formal Comment Period Open through January 25, 2017
Ballot Pools Open for Additional Members through January 10, 2017

Now Available

A 45-day formal comment period is open through **8 p.m. Eastern, Wednesday, January 25, 2017** for:

1. **CIP-003-7(i) - Cyber Security – Security Management Controls**
2. **CIP-003-7(i) Implementation Plan**
3. **Transient Cyber Asset (TCA) – Proposed revised definition**
4. **Removable Media – Proposed revised definition**
5. **CIP-003-7(i) Non-binding Poll**

Commenting

Use the electronic form to submit comments. If you experience any difficulties using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

Ballot Pools

The existing CIP-003-7 (LERC) ballot pool was used for all of the ballots associated with this portion of the project. The ballot pools have been re-opened to allow stakeholders to join if they are not existing members. The ballot pools are open through **8 p.m. Eastern, Tuesday, January 10, 2017.** Registered Ballot Body members may join the ballot pools here.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Initial ballots for the standard, implementation plan, and the two proposed revised definitions, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **January 16-25, 2017**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Al McMeekin (via email) or at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/76)
Ballot Name: 2016-02 Modifications to CIP Standards CIP-003-7(i) IN 1 ST
Voting Start Date: 1/16/2017 12:01:00 AM
Voting End Date: 1/25/2017 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 284
Total Ballot Pool: 365
Quorum: 77.81
Weighted Segment Value: 81.3

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	91	1	58	0.866	9	0.134	0	3	21
Segment: 2	7	0.1	1	0.1	0	0	0	2	4
Segment: 3	79	1	50	0.82	11	0.18	0	3	15
Segment: 4	27	1	14	0.667	7	0.333	0	0	6
Segment: 5	87	1	55	0.846	10	0.154	0	2	20
Segment: 6	57	1	35	0.761	11	0.239	0	1	10
Segment: 7	3	0.1	1	0.1	0	0	0	0	2
Segment: 8	3	0.3	3	0.3	0	0	0	0	0
Segment: 9	2	0.1	0	0	1	0.1	0	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.5	5	0.5	0	0	0	2	2
Totals:	365	6.1	222	4.959	49	1.141	0	13	81

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Third-Party Comments
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		None	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Third-Party Comments
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Devin Elverdi		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	None	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		None	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		None	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Third-Party Comments
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Abstain	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		None	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		None	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		None	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Negative	Third-Party Comments
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Cowlitz County PUD	Russell Noble		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	Comments Submitted
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	None	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Kissimmee Utility Authority	Anthony Darnell		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Negative	Comments Submitted
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Affirmative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		None	N/A
4	Austin Energy	Tina Garvey		Negative	Third-Party Comments
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	Comments Submitted
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Negative	Comments Submitted
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	LaGen	Richard Comeaux		Negative	Comments Submitted
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	Comments Submitted
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Jeanie Doty		Negative	Third-Party Comments
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Third-Party Comments
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Cowlitz County PUD	Ron Sporseen		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	None	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Affirmative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	Third-Party Comments
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments
5	Lincoln Electric System	Kayleigh Wilkerson		None	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer	Tim Womack	Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons		Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Negative	Third-Party Comments
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Black Hills Corporation	Eric Scherr		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		None	N/A
6	Entergy	Julie Hall		Negative	Comments Submitted
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	Comments Submitted
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	None	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Third-Party Comments
6	Omaha Public Power District	Joel Robles		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		None	N/A
6	Santee Cooper	Michael Brown		Affirmative	N/A
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Elizabeth Davis		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		None	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Abstain	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		None	N/A

Previous 1 Next

Showing 1 to 365 of 365 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/76)
Ballot Name: 2016-02 Modifications to CIP Standards CIP-003-7(i) Implementation Plan IN 1 OT
Voting Start Date: 1/16/2017 12:01:00 AM
Voting End Date: 1/25/2017 8:00:00 PM
Ballot Type: OT
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 280
Total Ballot Pool: 365
Quorum: 76.71
Weighted Segment Value: 87.87

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	91	1	60	0.896	7	0.104	0	3	21
Segment: 2	7	0.1	1	0.1	0	0	0	2	4
Segment: 3	79	1	54	0.885	7	0.115	0	3	15
Segment: 4	27	1	17	0.81	4	0.19	0	0	6
Segment: 5	87	1	58	0.906	6	0.094	0	2	21
Segment: 6	57	1	38	0.864	6	0.136	0	1	12
Segment: 7	3	0.1	1	0.1	0	0	0	0	2
Segment: 8	3	0.3	3	0.3	0	0	0	0	0
Segment: 9	2	0.1	0	0	1	0.1	0	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.5	5	0.5	0	0	0	1	3
Totals:	365	6.1	237	5.36	31	0.74	0	12	85

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Third-Party Comments
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		None	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Third-Party Comments
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Devin Elverdi		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	None	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Negative	Comments Submitted
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		None	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		None	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Abstain	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		None	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		None	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		None	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Cowlitz County PUD	Russell Noble		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	Comments Submitted
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	None	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Kissimmee Utility Authority	Anthony Darnell		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Negative	Comments Submitted
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Affirmative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		None	N/A
4	Austin Energy	Tina Garvey		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	Comments Submitted
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Negative	Comments Submitted
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Michael Ward		Affirmative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Cowlitz County PUD	Ron Sporseen		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	None	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Affirmative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	Third-Party Comments
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments
5	Lincoln Electric System	Kayleigh Wilkerson		None	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer	Tim Womack	Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons		Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		None	N/A
6	Entergy	Julie Hall		Negative	Comments Submitted
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	Comments Submitted
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	None	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Third-Party Comments
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		None	N/A
6	Santee Cooper	Michael Brown		Affirmative	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Elizabeth Davis		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		None	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		None	N/A

Previous 1 Next

Showing 1 to 365 of 365 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/76)
Ballot Name: 2016-02 Modifications to CIP Standards Transient Cyber Asset | New Definition IN 1 DEF
Voting Start Date: 1/16/2017 12:01:00 AM
Voting End Date: 1/25/2017 8:00:00 PM
Ballot Type: DEF
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 282
Total Ballot Pool: 365
Quorum: 77.26
Weighted Segment Value: 86.75

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	91	1	61	0.91	6	0.09	0	3	21
Segment: 2	7	0.1	1	0.1	0	0	0	2	4
Segment: 3	79	1	53	0.869	8	0.131	0	3	15
Segment: 4	27	1	16	0.762	5	0.238	0	0	6
Segment: 5	87	1	58	0.906	6	0.094	0	2	21
Segment: 6	57	1	38	0.844	7	0.156	0	1	11
Segment: 7	3	0.1	1	0.1	0	0	0	0	2
Segment: 8	3	0.3	3	0.3	0	0	0	0	0
Segment: 9	2	0.1	0	0	1	0.1	0	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.5	5	0.5	0	0	0	2	2
Totals:	365	6.1	236	5.292	33	0.808	0	13	83

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Third-Party Comments
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		None	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Third-Party Comments
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Devin Elverdi		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	None	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		None	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		None	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Abstain	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		None	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		None	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		None	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Negative	Third-Party Comments
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Cowlitz County PUD	Russell Noble		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	Comments Submitted
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	None	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Kissimmee Utility Authority	Anthony Darnell		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Negative	Comments Submitted
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Affirmative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		None	N/A
4	Austin Energy	Tina Garvey		Negative	Third-Party Comments
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	Comments Submitted
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Negative	Comments Submitted
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Michael Ward		Affirmative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Third-Party Comments
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Cowlitz County PUD	Ron Sporseen		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	None	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Affirmative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	Third-Party Comments
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments
5	Lincoln Electric System	Kayleigh Wilkerson		None	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer	Tim Womack	Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A
5	SunPower	Bradley Collard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons		Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Negative	Third-Party Comments
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		None	N/A
6	Entergy	Julie Hall		Negative	Comments Submitted
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	Comments Submitted
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	None	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		None	N/A
6	Santee Cooper	Michael Brown		Affirmative	N/A
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Affirmative	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Elizabeth Davis		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		None	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Abstain	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		None	N/A

Previous 1 Next

Showing 1 to 365 of 365 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/76)
Ballot Name: 2016-02 Modifications to CIP Standards Removable Media | New Definition IN 1 DEF
Voting Start Date: 1/16/2017 12:01:00 AM
Voting End Date: 1/25/2017 8:00:00 PM
Ballot Type: DEF
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 280
Total Ballot Pool: 365
Quorum: 76.71
Weighted Segment Value: 86.47

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	91	1	61	0.91	6	0.09	0	3	21
Segment: 2	7	0.1	1	0.1	0	0	0	2	4
Segment: 3	79	1	53	0.869	8	0.131	0	3	15
Segment: 4	27	1	16	0.762	5	0.238	0	0	6
Segment: 5	87	1	56	0.889	7	0.111	0	2	22
Segment: 6	57	1	38	0.844	7	0.156	0	1	11
Segment: 7	3	0.1	1	0.1	0	0	0	0	2
Segment: 8	3	0.3	3	0.3	0	0	0	0	0
Segment: 9	2	0.1	0	0	1	0.1	0	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.5	5	0.5	0	0	0	1	3
Totals:	365	6.1	234	5.275	34	0.825	0	12	85

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Third-Party Comments
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		None	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Third-Party Comments
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Devin Elverdi		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	None	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		None	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		None	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Abstain	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		None	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		None	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		None	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Negative	Third-Party Comments
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Cowlitz County PUD	Russell Noble		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	Comments Submitted
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	None	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Kissimmee Utility Authority	Anthony Darnell		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Negative	Comments Submitted
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Affirmative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		None	N/A
4	Austin Energy	Tina Garvey		Negative	Third-Party Comments
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	Comments Submitted
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Negative	Comments Submitted
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Michael Ward		Affirmative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Jeanie Doty		Negative	Third-Party Comments
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Third-Party Comments
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Cowlitz County PUD	Ron Sporseen		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	None	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Affirmative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	Third-Party Comments
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments
5	Lincoln Electric System	Kayleigh Wilkerson		None	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer	Tim Womack	Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A
5	SunPower	Bradley Collard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons		Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Negative	Third-Party Comments
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		None	N/A
6	Entergy	Julie Hall		Negative	Comments Submitted
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	Comments Submitted
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	None	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		None	N/A
6	Santee Cooper	Michael Brown		Affirmative	N/A
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Affirmative	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Elizabeth Davis		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		None	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		None	N/A

Previous 1 Next

Showing 1 to 365 of 365 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/76)
Ballot Name: 2016-02 Modifications to CIP Standards CIP-003-7(i) Non-binding Poll IN 1 NB
Voting Start Date: 1/16/2017 12:01:00 AM
Voting End Date: 1/26/2017 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 277
Total Ballot Pool: 361
Quorum: 76.73
Weighted Segment Value: 79.74

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	90	1	47	0.839	9	0.161	12	22
Segment: 2	7	0.1	1	0.1	0	0	2	4
Segment: 3	78	1	42	0.808	10	0.192	11	15
Segment: 4	27	1	10	0.625	6	0.375	5	6
Segment: 5	86	1	43	0.811	10	0.189	10	23
Segment: 6	56	1	29	0.744	10	0.256	8	9
Segment: 7	3	0.1	1	0.1	0	0	0	2
Segment: 8	3	0.3	3	0.3	0	0	0	0
Segment: 9	2	0.1	0	0	1	0.1	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	9	0.5	5	0.5	0	0	2	2
Totals:	361	6.1	181	4.827	46	1.273	50	84

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		None	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Devin Elverdi		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Abstain	N/A
1	Duke Energy	Doug Hils		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Danny Pudenz		Abstain	N/A
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		None	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		None	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A
1	Platte River Power Authority	Matt Thompson		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Abstain	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		None	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Abstain	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa	Michael Watkins	None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Abstain	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		None	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		None	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		None	N/A
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		None	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Negative	Comments Submitted
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Abstain	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Abstain	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	Comments Submitted
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Kissimmee Utility Authority	Anthony Darnell		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Negative	Comments Submitted
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Abstain	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Abstain	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Abstain	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Xcel Energy, Inc.	Michael Ibold		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		None	N/A
4	Austin Energy	Tina Garvey		Negative	Comments Submitted
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	Comments Submitted
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Negative	Comments Submitted
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Abstain	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	LaGen	Richard Comeaux		Negative	Comments Submitted
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Abstain	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Abstain	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Michael Ward		Abstain	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Matthew Finn		Affirmative	N/A
5	Austin Energy	Jeanie Doty		Negative	Comments Submitted
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Comments Submitted
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Cowlitz County PUD	Ron Sporseen		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Abstain	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Affirmative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	Comments Submitted
5	Lakeland Electric	Jim Howard		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		None	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Negative	Comments Submitted
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Abstain	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Abstain	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Negative	Comments Submitted
5	Ontario Power Generation Inc.	David Ramkalawan		Abstain	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Platte River Power Authority	Tyson Archie		None	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Abstain	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer	Tim Womack	Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	Seattle City Light	Mike Haynes		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	TECO - Tampa Electric Co.	R James Rocha		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		None	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Abstain	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		None	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons		Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Negative	Comments Submitted
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Entergy	Julie Hall		Negative	Comments Submitted
6	Exelon	Becky Webb		Abstain	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	Comments Submitted
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Abstain	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Comments Submitted
6	Omaha Public Power District	Joel Robles		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Abstain	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		None	N/A
6	Santee Cooper	Michael Brown		Abstain	N/A
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Abstain	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Elizabeth Davis		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		None	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	Comments Submitted
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		None	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		None	N/A

Previous 1 Next

Showing 1 to 361 of 361 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards
CIP-003-7(i)

Formal Comment Period Open through January 25, 2017
Ballot Pools Open for Additional Members through January 10, 2017

Now Available

A 45-day formal comment period is open through **8 p.m. Eastern, Wednesday, January 25, 2017** for:

1. **CIP-003-7(i) - Cyber Security – Security Management Controls**
2. **CIP-003-7(i) Implementation Plan**
3. **Transient Cyber Asset (TCA) – Proposed revised definition**
4. **Removable Media – Proposed revised definition**
5. **CIP-003-7(i) Non-binding Poll**

Commenting

Use the electronic form to submit comments. If you experience any difficulties using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

Ballot Pools

The existing CIP-003-7 (LERC) ballot pool was used for all of the ballots associated with this portion of the project. The ballot pools have been re-opened to allow stakeholders to join if they are not existing members. The ballot pools are open through **8 p.m. Eastern, Tuesday, January 10, 2017.** Registered Ballot Body members may join the ballot pools here.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Initial ballots for the standard, implementation plan, and the two proposed revised definitions, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **January 16-25, 2017**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Al McMeekin (via email) or at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | CIP-003-7(i), Implementation Plan, and definition of TCA and Removable Media
Comment Period Start Date:	12/12/2016
Comment Period End Date:	1/25/2017
Associated Ballots:	2016-02 Modifications to CIP Standards CIP-003-7(i) Implementation Plan IN 1 OT 2016-02 Modifications to CIP Standards CIP-003-7(i) IN 1 ST 2016-02 Modifications to CIP Standards CIP-003-7(i) Non-binding Poll IN 1 NB 2016-02 Modifications to CIP Standards Removable Media | New Definition IN 1 DEF 2016-02 Modifications to CIP Standards Transient Cyber Asset | New Definition IN 1 DEF

There were 60 sets of responses, including comments from approximately 50 different people from approximately 46 companies representing 9 of the Industry Segments as shown in the table on the following pages.

Questions

1. Definition: The SDT revised the definition of Transient Cyber Asset such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

2. Definition: The SDT revised the definition of Removable Media such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

3. Requirement R2: The SDT revised CIP-003-7(i), Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to mitigate the risk of propagation of malware from transient devices. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

4. Attachment 2: The SDT revised the evidential language of CIP-003-7(i), Attachment 2, Section 5 to make the Measures consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides examples of temporarily connected devices, and strategies to consider in developing the Transient Cyber Asset and Removable Media malicious code mitigation plan(s) at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

6. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

7. If you have additional comments on the proposed revisions to address the FERC directive regarding TCAs for low impact BES Cyber Systems that you have not provided in response to the questions above, please provide them here.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Luminant - Luminant Energy	Brenda Hampton	6		Luminant	Brenda Hampton	Luminant - Luminant Energy	6	Texas RE
					Stewart Rake	Luminant Mining Company LLC	7	Texas RE
					Alshare Hughes	Luminant - Luminant Generation Company LLC	5	Texas RE
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
ACES Power Marketing	Brian Van Gheem	6	NA - Not Applicable	ACES Standards Collaborators	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	RF
					Shari Heino	Brazos Electric Power Cooperative, Inc.	1,5	Texas RE
					Ellen Watkins	Sunflower Electric Power Corporation	1	SPP RE
					Mark Ringhausen	Old Dominion Electric Cooperative	3,4	SERC
					Eric Jensen	Arizona Electric Power Cooperative, Inc.	1	WECC

					Ryan Strom	Buckeye Power, Inc.	4	RF
					Susan Sosbe	Wabash Valley Power Association	3	RF
Chris Gowder	Chris Gowder		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utility Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steve Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Mark Brown	City of Winter Park	4	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	9	FRCC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Southern Company - Southern	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC

Company Services, Inc.					R. Scott Moore	Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,10	NPCC	RSC no Dominion and OPG	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					MIchael Forte	Con Edison	1	NPCC

					Quintin Lee	Eversource Energy	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Chuck Lawrence	American Transmission Company	1	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Power	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Jeremy Volls	Basin Electric Power Coop	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO

					Mike Morrow	Midcontinent Independent System Operator	2	MRO
Colorado Springs Utilities	Shannon Fair	6		Colorado Springs Utilities	Kaleb Brimhall	Colorado Springs Utilities	5	WECC
					Charlie Morgan	Colorado Springs Utilities	3	WECC
					Shawna Speer	Colorado Springs Utilities	1	WECC
					Shannon Fair	Colorado Springs Utilities	6	WECC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Megan Wagner	Westar Energy	1,3,5,6	SPP RE
					Robert Gray	Board of Public Utilities (Kansas-BPU)	3	SPP RE
					Steve Keller	Southwest Power Pool Inc.	2	SPP RE
					Tony Eddleman	Nebraska Public Power District	1,3,5	SPP RE
Santee Cooper	Shawn Abrams	1		Santee Cooper	Tom Abrams	Santee Cooper	1	SERC
					Rene' Free	Santee Cooper	1	SERC
					Chris Jimenez	Santee Cooper	1	SERC
					Paul Camilletti	Santee Cooper	5	SERC
					Bob Rhett	Santee Cooper	5	SERC
					Mike Frederick	Santee Cooper	1	SERC
					Troy Lee	Santee Cooper	1	SERC

1. Definition: The SDT revised the definition of Transient Cyber Asset such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	

Seattle City Light has concerns that the revised definition of Transient Cyber Asset is not consistent with the risk-based approach reflected in the NERC CIP version 5/6 Standards. In particular Seattle finds the revised definition is inconsistent with the language of CIP-002-5.1 R1.3 regarding identification of BES Cyber Systems (and by extension BES Cyber Assets) at Low impact facilities, specifically that: “a discrete list of low impact BES Cyber Systems is not required.” Given that the proposed definition defines Transient Cyber Assets in terms of BES Cyber Assets and BES Cyber Systems, Seattle does not understand how the existence of any low impact Transient Cyber Asset can be documented or audited absent a list of such BES Cyber Systems or Assets. Seattle is further concerned that the revised definition could lead to a requirement to produce such lists, which previously has been deemed not consistent with the risk-based approach adopted in CIP version 5/6 (because the development and accurate maintenance of such lists would consume large resources that would provide greater benefits to cyber security if applied elsewhere). At this time Seattle does not have alternative language to suggest to resolve this conundrum, which is inherent to the structure of CIP version 5/6. Perhaps a revision of the definition for Low impact Transient Cyber Asset to reference only a temporary connection “to a BES Cyber System at a low impact facility” might work, but Seattle remains unconvinced that such a definition would prove auditable.

Likes 0	
Dislikes 0	
Response	

Julie Hall - Entergy - 6	
Answer	No
Document Name	
Comment	

The proposed definition of Transient Cyber Asset (TCA) implies additional requirements for entities to comply with that is in misalignment with standards that are currently approved and in effect. The purpose of CIP-003-7(i) is to create TCA requirements for Low Impact BES Cyber Systems, yet none of the criteria of item 4 of the definition can be achieved for Lows without imposing additional, and improper, requirements upon the Registered Entities. Item 4 bullets 2 and 3 are omitted because they explicitly require the device or network to be associated with a high or medium impact, leaving just the direct connection to a BES Cyber Asset as the required #4 criteria. However, CIP-002-5.1 R1.3 reads “Identify each asset that contains a low impact BES Cyber System according…if any (a discrete list of low impact BES Cyber Systems is not required).” The requirement explicitly states that a discrete list of BES Cyber Systems is not required. BES Cyber Systems are defined as “One or more BES Cyber Assets logically grouped”, showing that BES Cyber Assets are a sub-componet of a BES Cyber System. CIP-002-5.1 explicitly states that a list of low impact BCS is not required, yet this definition of TCA would require entities to evaluate and inventory, and maintain that inventory, to identify every BES Cyber Asset in order to correctly identify TCA that could be used at a low impact site. Entergy proposes some verbiage to include low impact BCS, while not adding additional inventorying requirements such as “Anticipated for use within a low impact BCS, if any”.

Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
Since PCA is already defined by NERC, NRG recommends deleting associated with high or medium impact BES Cyber Systems since “associated” could be misunderstood and appears to be redundant. For example, would a VPN connection be considered a TCA? (i.e. connecting at layer 3 or below)	
Likes 0	
Dislikes 0	
Response	
Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
1. We feel the SDT’s approach to revise the definition of Transient Cyber Assets (TCA), such that it is relevant to the controls required for high, medium, and low impact BES Cyber Systems, is inconsistent with the directives listed within FERC Order No. 822. These directives focus on the high and medium impact BES Cyber Security requirements. However, the proposed revisions implicitly require low impact entities to have the same level of risk mitigations in places as if they were associated with high and medium impact BES Cyber Systems. We believe the SDT should avoid the inclusion of low impact BES Cyber Systems entirely or provide proof of a risk analysis to substantiate this activity. 2. The SDT’s proposed approach will also create difficulty for industry to demonstrate compliance since a BES Cyber System’s inventory list is not required for low impact entities. How are auditors able to benchmark a low impact entity’s compliance program without a current list? 3. We suggest the SDT consider another method to address the FERC directive that still preserves the low impact requirements and the explicit exclusion from being required to have an inventory list of low impact assets. Such an approach could include TCAs in the technical guidance under Electronic Access Controls. 4. Another possible approach is for low impact entities to have a documented process that applies electronic access controls for TCAs to low impact assets. i. Auditors could verify that the entity has developed the documented process, and the entity could demonstrate compliance by providing the document as evidence. ii. This approach also preserves the disparate treatment of low and medium impact assets by assigning different requirement levels that commensurate with BES level risks.	
Likes 0	
Dislikes 0	
Response	

Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	
Comment	
Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Transient Cyber Asset definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified. The definition does not spell out what defines a TCA in a low impact environment. Should the definition include additional instruction related to item 4 such as "connected to a cyber asset located in an asset contiaing low impact BES Cyber Systems"?	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	No
Document Name	
Comment	
In the current TCA definition, section 4, first bullet: If the intent of the definition for "BES Cyber Asset" to be applicable for all three impact classifications (High, Medium, and Low), then SDG&E recommends adding this clarification.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Transient Cyber Asset definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.	
Likes 0	

Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy would like to point out a possible typo on page 3 of the Proposed Definitions of: Transient Cyber Asset"(TCA) and "Removable Media" document. The title of the section on page 3 reads "Currently Approved Definition of Transient Cyber Asset (TCS)". The definition below is actually the definition of Removable Media. The title appears to be incorrect. We recommend the drafting team change the title to read: *"Currently Approved Definition of Removable Media".*	
Likes 0	
Dislikes 0	
Response	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	

Dislikes 0	

Response

Roger Dufresne - Hydro-Qu?bec Production - 5

Answer	Yes
Document Name	

Comment

Add a « Low impact BES » item in the TCA definition. This will exempt the inventory requirement for low to demonstrate compliance for the TCA.

The proposed definition of a Transient Cyber Asset (TCA) is:

A Cyber Asset that is:

1. capable of transmitting or transferring executable code,

2. not included in a BES Cyber System,

3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and

4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:

BES Cyber Asset,

Add "Low impact BES Cyber System",

network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or

PCA associated with high or medium impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

It would be helpful if the revised definitions could be reorganized to provide the inclusions first and the exclusions second to make them easier to read and implement. For example, the TCA definition could be changed to:

“A Cyber Asset that is: 1) capable of transmitting or transferring executable code; 2) directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: BES Cyber Asset, network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or PCA associated with high or medium impact BES Cyber Systems; 3) not included in a BES Cyber System; and 4) not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems. Examples...”

Also, the applicability of the definitions to LIBCS is not clear, we recommend changing “BES Cyber Asset” in bullet 4 for each definition to “BES Cyber System” or alternatively “low, medium, or high impact BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	Yes
Document Name	

Comment

Suggest to add a « Low impact BES » item in the TCA definition. This will exempt the inventory requirement for low to demonstrate compliance for the TCA.

The proposed definition of a Transient Cyber Asset (TCA) is:

A Cyber Asset that is:

1. *capable of transmitting or transferring executable code,*
2. *not included in a BES Cyber System,*
3. *not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and*
4. *directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:*

- *BES Cyber Asset,*
- *Add “Low impact BES Cyber System”,*
- *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
- *PCA associated with high or medium impact BES Cyber Systems.*

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Santee Cooper agrees with APPA's comment/concern.	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Transient Cyber Asset definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobby Olsen - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Anctil - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Definition: The SDT revised the definition of Removable Media such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov

Answer	No
Document Name	

Comment

In the proposed Removable Media definition, section 4, first bullet: If the intent of the definition for “BES Cyber Asset” to be applicable for all three impact classifications (High, Medium, and Low), then SDG&E recommends adding this clarification.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 3

Answer	No
Document Name	

Comment

Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP’s and PCA’s to the Removable Media definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified. The definition does not spell out what defines RMin a low impact environment. Should the definition include additional instruction related to item 4 such as “connected to a cyber asset located in an asset contiaing low impact BES Cyber Systems”?

Likes 0	
Dislikes 0	

Response

Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators

Answer	No
Document Name	

Comment

1. Similar to TCAs, we suggest the SDT revise its approach and remove low impact BES Cyber Security requirements from the definition of Removable Media (RM). We feel its relevance on controls required for high, medium, and low impact BES Cyber Systems is not the best way to address the directives listed in FERC Order No. 822. The proposed revisions implicitly require low impact entities to have the same level of risk mitigiations in places as if they were associated with high and medium impact BES Cyber Systems. We believe the SDT should avoid the inclusion of low impact BES Cyber Systems entirely or provide proof of a risk analysis to substatntiate this activity.
2. We suggest the SDT consider another method to address the FERC directive that still preserves the low impact requirements and the explicit exclusion from being required to have an inventory list of low impact assets. Such an approach could include Removable Media in the technical guidance under Electronic Access Controls that are currently approved.
3. One possible approach is for low impact entities to have a documented process that applies electronic access controls for Removable Media to low impact assets.
    i. Auditors could verify that the entity has developed the documented process, and the entity could demonstrate compliance by providing the document as evidence.
    ii. This approach also preserves the disparate treatment of low and medium impact assets by assigning different requirement levels that commensurate with BES level risks

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

Since PCA is already defined by NERC, NRG recommends deleting associated with high or medium impact BES Cyber Systems since “associated” could be misunderstood and appears to be redundant.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6

Answer	No
Document Name	

Comment

The proposed definition of Removable Media (RM) implies additional requirements for entities to comply with that is in misalignment with standards that are currently approved and in effect. The purpose of CIP-003-7(i) is to create RM requirements for Low Impact BES Cyber Systems, yet none of the criteria of item 4 of the definition can be achieved for Lows without imposing additional, and improper, requirements upon the Registered Entities. Item 4 bullets 2 and 3 are omitted because they explicitly require the device or network to be associated with a high or medium impact, leaving just the direct connection to a BES Cyber Asset as the required #4 criteria. However, CIP-002-5.1 R1.3 reads “Identify each asset that contains a low impact BES Cyber System according…if any (a discrete list of low impact BES Cyber Systems is not required).” The requirement explicitly states that a discrete list of BES Cyber Systems is not required. BES Cyber Systems are defined as “One or more BES Cyber Assets logically grouped”, showing that BES

Cyber Assets are a sub-componet of a BES Cyber System. CIP-002-5.1 explicitly states that a list of low impact BCS is not required, yet this definition of TCA would require entities to evaluate and inventory, and maintain that inventory, to identify every BES Cyber Asset in order to correctly identify RM that could be used at a low impact site. Entergy proposes some verbiage to include low impact BCS, while not adding additional inventorying requirements such as “Anticipated for use within a low impact BCS, if any”.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

As is the case for the revised Transiet Cyber Asset definition, Seattle City Light has concerns that the revised definition of Removable Media is not consistent with the risk-based approach reflected in the NERC CIP version 5/6 Standards. In particular Seattle finds the revised definition is inconsistent with the language of CIP-002-5.1 R1.3 regarding identification of BES Cyber Systems (and by extension BES Cyber Assets) at Low impact facilities, specifically that: “a discrete list of low impact BES Cyber Systems is not required.” Given that the proposed definition defines Removable Media in terms of BES Cyber Assets and BES Cyber Systems, Seattle does not understand how the existence of any low impact Removable Media can be documented or audited absent a list of such BES Cyber Systems or Assets. Seattle is further concerned that the revised definition could lead to a requirement to produce such lists, which previously has been deemed not consistent with the risk-based approach adopted in CIP version 5/6 (because the development and accurate maintenance of such lists would consume large resources that would provide greater benefits to cyber security if applied elsewhere). At this time Seattle does not have alternative language to suggest to resolve this conundrum, which is inherent to the structure of CIP version 5/6. Perhaps a revision of the definition for Low impact Removable Media to reference only a temporary connection “to a BES Cyber System at a low impact facility” might work, but Seattle remains unconvinced that such a definition would prove auditable.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	Yes
Document Name	

Comment

Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Removable Media definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment

Santee Cooper agrees with APPA's comment/concern.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	Yes
Document Name	

Comment

Suggest to dd a « Low impact BES » item in the TCA definition. This will exempt the inventory requirement for low to demonstrate compliance for the TCA.

The proposed definition of Removable Media is:

Storage media that:

1. *are not Cyber Assets,*
2. *are capable of transferring executable code,*
3. *can be used to store, copy, move, or access data, and*
4. *are directly connected for 30 consecutive calendar days or less to a:*
    - *BES Cyber Asset,*

- *Low impact BES Cyber System,*
- *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
- *Protected Cyber Asset associated with high or medium impact BES Cyber Systems.*

Likes 0	
Dislikes 0	

Response

Roger Dufresne - Hydro-Qu?bec Production - 5

Answer	Yes
Document Name	

Comment

Add a « Low impact BES » item in the TCA definition. This will exempt the inventory requirement for low to demonstrate compliance for the TCA.

The proposed definition of Removable Media is:

Storage media that:

5. *are not Cyber Assets,*

6. *are capable of transferring executable code,*

7. c*an be used to store, copy, move, or access data, and*

8. are directly *connected for 30 consecutive calendar days or less to a:*

BES Cyber Asset,

Low impact BES Cyber System,

network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or

Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer	Yes
Document Name	

Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Removable Media definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes

Document Name	
Comment	
The term “transferring code” is misleading because the device itself (for example, storage media) cannot transfer code without assistance from the host computer.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Anctil - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobby Olsen - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE noticed the TCA definition includes examples of what directly connected means, "*directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a*".

There are no examples for "directly connected" listed in the Removable Media definition. Texas RE recommends that the SDT provide examples to provide clarity to the industry. There are instances when removable media may be physically directly connected but not active until mounted.

Likes 0	
Dislikes 0	
Response	

3. Requirement R2: The SDT revised CIP-003-7(i), Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to mitigate the risk of propagation of malware from transient devices. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The NSRF clearly understands that all entities regardless of size can be the door way for malicious code to entire into the BES systems. This includes small entities with one Low Impact BES Cyber Systems only (read low risk) (maybe a generator, one Transmission sub station, or control system). With this is mind, the NSRF has the following concerns that the SDT should clarify for all entities with Low Impact BES Cyber Systems.

The NSRF has concerns with Attachment 1, part 5.2 for entities that have Low Impact BES Cyber Systems, only. The actionable items in 5.2 is for us the entity to “Review” items that the “other party” needs to do to do prior to connecting to our Low Impact BES Cyber System. Please clariy what “review” means? What is acceptable within our review process? Attachment 2 states examples of electronic mail, policies, contracts, etc. Do we just review that the “other party” states that they will accomplish the attributes of 5.2 and have that stated within a contract, e-mail, STOW, etc. and we are compliant? This will play a role with proprietary software when a vendor will not provide associated evidence.

This clarity will reduce the compliance risks for the small entity and will assure that entities meet the attributes of 5.2, thus maintaining a secure BPS.

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

• Antivirus software, including manual or managed updates of signatures or patterns;

• Application whitelisting; or

• Other method(s) to mitigate the introduction of malicious code.

Please clarify how the SDT wishes to use the semicolon within the first bullet of 5.1? Does this mean “and” or “or” as in the second bullet? We have the same question for all semicolons in 5.2 as well. The NSRF believes by adding a simple “or” after each semicolon, we will clearly know what the intent of the bulleted items are.

Likes 1	Georgia Transmission Corporation, 1, Snodgrass Jason
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	
Comment	

The language is open ended and fails to provide discrete direction to entities on how to implement a plan. This will lead to subjective enforcement, with the possibility for significant discrepancies and differences between regions.

Likes 0	
Dislikes 0	
Response	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	
Comment	

Seattle City Light agrees with the revisions so far as they go, but finds that they do not address the question of what would be acceptable evidence of the existence of any Low impact Transient Cyber Asset (based on the proposed definition) in the absence of an explicit list of Low impact BES Cyber Systems and Assets at a facility. As discussed in the definition comment above, Seattle does not have a solution to the problem, which is inherent to the structure of CIP verion 5/6.

Likes 0	
Dislikes 0	
Response	

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	
Comment	

This is a low impact requirement rather than a high or medium impact requirement. While risks of malicious code are definitely present, the reduced risk level would make this entire requirement more effective by requiring the entity document and implement a security program with appropriate controls that prevent introduction of malicious code. Examples of appropriate controls are: application whitelisting, antivirus, use of bootable CDs without known malware, contracts with vendors, etc. Note that use of third party TCA is expected to be much more frequent on low impact BCS and highly presecriptive requirements are less effective.

Should the above approach not be acceptable, requirement 5.3.1 and 5.3.2 should be consolidated into a single statement. A requirement to scan prior to connecting and then separately document and mitigate is redundant. The Removable media simply needs to be clean prior to connecting to a Transient Cyber Asset. Seminole suggests making that the requirement.

For example, the language could be modified to state:

For Removable Media, document and implement methods that prevent the introduction of malicious code on BES Cyber Assets when connecting Removable Media. In cases of detected malicious code that cannot be removed, the entity shall document how the identified malware is mitigated.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns

Answer	No
Document Name	

Comment

ITC Holdings agrees with the comment submitted by NSRF – see below:

The NSRF clearly understands that all entities regardless of size can be the door way for malicious code to entire into the BES systems. This includes small entities with one Low Impact BES Cyber Systems only (read low risk) (maybe a generator, one Transmission sub station, or control system). With this is mind, the NSRF has the following concerns that the SDT should clarify for all entities with Low Impact BES Cyber Systems.

The NSRF has concerns with Attachment 1, part 5.2 for entities that have Low Impact BES Cyber Systems, only. The actionable items in 5.2 is for us the entity to “Review” items that the “other party” needs to do to do prior to connecting to our Low Impact BES Cyber System. Please clariy what “review” means? What is acceptable within our review process? Attachment 2 states examples of electronic mail, policies, contracts, etc. Do we just review that the “other party” states that they will accomplish the attributes of 5.2 and have that stated within a contract, e-mail, STOW, etc. and we are compliant? This will play a role with proprietary software when a vendor will not provide associated evidence.

This clarity will reduce the compliance risks (burden) for the small entity and will assure that entities meet the attributes of 5.2.

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

• Antivirus software, including manual or managed updates of signatures or patterns;

• Application whitelisting; or

• Other method(s) to mitigate the introduction of malicious code.

Please clarify how the SDT wishes to use the semicolon within the first bullet of 5.1? Does this mean “and” or “or” as in the second bullet? We have the same question for all semicolons in 5.2 as well. The NSRF believes by adding a simple “or” after each semicolon, we will clearly know what the intent of the bulleted items are.	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
MMWEC supports the comments submitted by Georgia Transmission Corp. regarding streamling Section 5 by moving the bullets to GTB and keeping the security objective in the Attachment.	
Likes 0	
Dislikes 0	
Response	
Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
1. We have concerns with part 5.2 of Attachment 1 for applicable entities that only have Low Impact BES Cyber Systems. Many of these entities provide a small risk to the BES since they only have one low impact BES Cyber Systems (e.g. a generator, one Transmission substation, or a single control system). Will Regional Entities conduct the same audit for small entities as they would for large multi-regional corporate companies? What is the impact when a vendor does not comply with the request listed in part 5.2? 2. We also question the need for additional explicit requirements to validate vendor security and patch management plans as part of a low impact entity’s cyber security policies. We believe these requirements are already incorporated in an entity’s Electronic Access Controls Policy. These additional requirements are a burden to existing low impact entities that may only have one or two TCA-applicable or RM-applicable BES cyber assets. We recommend removing these requirements for low Impact entities until after the effective date for NERC Reliability Standard CIP-007-3 (i.e. September 1, 2018). 3. The inclusion of TCA and RM with the final definition of LERC is unnecessary. We don't agree with the SDT's approach of posting two options, and then recommend the all-inclusive option over the other. The SDT should wait for industry to provide feedback on both options or post only one path forward and determine if industry supports it. The one option adds additional risk for ballot approval.	
Likes 0	
Dislikes 0	

Response

Mike Anctil - Los Angeles Department of Water and Power - 3	
Answer	No
Document Name	
Comment	
This NERC project is adding a new Section 5 bringing into scope Transient Cyber Assets and Removable Media for Low Impact Facilities which is a much larger scope than our High and Medium Impact Program without any extension of time for compliance indicated for implementation. This will be impactful to the Power System.	
Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation appreciates the Standards Drafting Team's consideration of prior recommendations. Reclamation agrees with the changes and has the following question: In this version of CIP-003-7(i), did the SDT intend to add guidance regarding the new section on page 9 under Requirement 1 "1.2.6 Declaring and responding to CIP Exceptional Circumstances" in Attachment 1 and/or Attachment 2?	
Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE's appreciates the SDT's efforts to implement the FERC directive in Order No. 822 to "develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to the bulk electric system reliability." In implementing this directive, Texas RE notes that the SDT appears to have used the existing Transient Cyber Asset (TCA) and Removable Media requirements for medium and high impact BES Cyber Systems and associated Protected Cyber Assets set forth in CIP-10-2, Attachment 1, Sections 1 through 3 as the basis for developing the new TCA and removable media requirements for low impact BES Cyber Systems.

While Texas RE agrees with this general approach, Texas RE notes that the SDT elected to not include all applicable requirements. For instance, the current draft of CIP-003, Attachment 1, Section 5 omits any requirements to mitigate software vulnerabilities (CIP-10-2, Attachment 1, Section 1.3 for TCAs managed by the Responsible Entity; CIP-10-2, Attachment 1, Section 2.1 for TCAs managed by a party other than the Responsible Entity). **Texas RE requests that the SDT provide its risk-based justification for why those aspects of the CIP-010-2, Attachment 1 requirements for medium and high impact TCAs and removable media are not correspondingly extended to similar low impact devices. Among other things, this will assist Texas RE in its efforts to understand, evaluate, and ensure compliance with the new low impact requirements.**

In addition, Texas RE noticed the following:

- There is no distinction provided for Removable Media used by different parties. Was that the intent of the SDT? As written it appears to be for any Removable Media used by any party (e.g., vendor, or third party technician/personnel).

- Texas RE recommends that the SDT specifically address the impact of backup tapes, libraries, and drives. More specifically Texas RE recommends addressing magnetic tapes, in regard to section 5.3.2. How would an entity mitigate the threat of detected malicious code on magnetic tapes prior to connecting it to a high, medium, or low impact BES Cyber System?

- On Page 29, Section 5 - Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation; there is an extra "_" that is not needed after the colon symbol.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

1) The bulleted list creates requirements that are too prescriptive. Use alternative language for Section 5.1 and 5.2 to remove the bullet points (because they may be used against you in some fashion in the future), and re-write the requirements. The bullet points should go into the GTB section so that there is less chance for a misinterpretation of reinterpretation that would require the implementation of more than one of the bulleted point inorder to meet compliance.

2) As written, the requirements listed for TCAs in CIP-003-7(i) for Low Impact assets is a subset of the requirements for high and medium impact included in CIP-010-2 R4. As is or if changed the GTB section should include a statement the low impact requirements are a subset of those for High and Medium.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6

Answer	Yes
Document Name	

Comment

Agree with CIP-003-7(i), Attachment 1, Section 5 as written in this draft. As written, this verbiage implies entities has latitude to implement a strategy based on a risk to achieve the goal of the standard. See response to question 4 below for concerns regarding actual implementation of plans.

Likes 1	Georgia Transmission Corporation, 1, Snodgrass Jason
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	Yes
Document Name	

Comment

Exelon supports the changes made to CIP-003-7(i), R2, Attachment 1, adding Section 5; however, we request the SDT consider the following adjustments:

1. The language in Attachment 1, Section 5, regarding “achieve the objective of mitigating the risk of the introduction of malicious code,” differs from the language in CIP-010-2, R4, Attachment 1, Section 1.3, which states “…achieves the objective of mitigating the introduction of…” Exelon requests the SDT consider aligning the two obligations to the language found in CIP-010-2, R4 or add clarification to the Guidelines and Technical Basis that provides clarity regarding the addition of “...the risk of…” and whether there are any additional or different

expectations for Responsible Entities related to CIP-003-7(i), R2. Exelon is concerned that the addition of "risk" could be interpreted to require performing and documenting a risk assessment of all of the risks posed by the introduction of malicious code.

The following sentence (or something comparative) could be added to the Guidelines and Technical Basis as the last sentence in the first paragraph related to Section 5.1 if the SDT determines the requirement language does not require alignment: "When determining the method(s) to mitigate the introduction of malicious code, it is not intended Responsible Entities have to perform and document a risk assessment to determine all of the risks associated with the introduction of malicious code."

1. Attachment 1, Section 5.3.2 states, "Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System." Exelon proposes a one-word change to replace the "…threat of…" to "…threat from…" This minor wording change helps to clarify the meaning of the obligation. Using the word "from" makes it clear that the mitigation of the threat is associated with already detected malicious code, as opposed to mitigation of a general threat of malicious code that may occur in the future.

Likes 0	
Dislikes 1	Georgia Transmission Corporation, 1, Snodgrass Jason

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities

Answer	Yes
Document Name	

Comment

1) The bulleted list creates requirements that are too prescriptive. Use alternative language for Section 5.1 and 5.2 to remove the bullet points (because they may be used against you in some fashion in the future), and re-write the requirements. The bullet points should go into the GTB section so that there is less chance for a misinterpretation of reinterpretation that would require the implementation of more than one of the bulleted point inorder to meet compliance.

2) As written, the requirements listed for TCAs in CIP-003-7(i) for Low Impact assets is a subset of the requirements for high and medium impact included in CIP-010-2 R4. As is or if changed the GTB section should include a statement the low impact requirements are a subset of those for High and Medium.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	Yes
Document Name	

Comment

Comments: Both sections 5.1 and 5.2 contain an option of "Other method(s) to mitigate the introduction of malicious code" which grants responsible entities flexibility in choosing alternative methods not included in the list of bulleted items as long as the methods achieve the core security objective

outlined in section 5. Therefore, it seems that emphasis is placed on achieving the security objective established by the core of section 5 and the distinction between 5.1 and 5.2 is for the plan to include and cover whom is managing TCAs and not specificly to capture the various options bulleted within the required plan.

As such, GTC believes the bullet point “options” introduces unneccesary prescriptive language and can be removed from the requirements without changing the intent of the requirement whatsoever and the drafting team could simplify with and affirmative ballot. GTC recognizes these options provide contextual ideas of how one could go about achieving the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems and further recommends that they be relocated into the guidelines and technical basis of the standard.

This streamlined revision to section 5 could be simplified for clarity of implementation on the front end and clarity of compliance testing on the audit end as follows:

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

5.1 Method(s) to mitigate the introduction of malicious code for Transient Cyber Asset(s) managed by the Responsible Entity, if any.

5.2 Method(s) to mitigate the introduction of malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any.

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

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

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

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy would like to see added clarification within the Guidelines and Technical Basis around the concept of an acceptable review of a 3rd party vendors malware mitigation mechanisms. Currently, in Section 5.2 of Attachment 1, a Responsible Entity is required to “Review” one or a combination of the malware mitigation mechanisms of a 3rd party vendor. Our concern is that it is unclear what constitutes an acceptable “review” of these mechanisms. It is possible that what is considered an acceptable review by one entity, may not be considered acceptable by another. We suggest the drafting team consider adding language to the Guidelines and Technical Basis further describing what constitutes an acceptable review.

Likes 0	
Dislikes 0	

Response

Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	Yes
Document Name	
Comment	
We like to see examples how to have the ability to restrict malware to the TCA's. Also like to see some examples around technical guidance and mitigation plans. Possibly adding administrative control methods in the technical basis sections for transient devices. Add language in the technical basis restricting movement of TCA's.	
Likes 0	
Dislikes 0	
Response	

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA. In Attachment 1, Section 5, 5.2, what frequency is intended by the words "prior to"? Is this intended to be once upon execution of a vendor/contractor support contract, or is it intended to be at some other interval/frequency?	
Likes 0	
Dislikes 0	
Response	

Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	

Summary of changes in page 44 of the guidelines CIP010 mentioned :

“All requirements related to TCA and RM are included within a single standard, CIP010. But requirements exist also in CIP-003-07 R2 . HQP suggest to modify the summary of changes.

The word “Managed” should be in lower case for paragraph in the page 56 of 62 “**Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity”**.

It could be usefull to introduce base of risk in the case of a TCA connected to LOW impact BES systems without external connectivity.

Likes 0	
Dislikes 0	
Response	

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	

Summary of changes in page 44 of the guidelines CIP010 mentioned :

“All requirements related to TCA and RM are included within a single standard, CIP010. But requirements exist also in CIP-003-07 R2 . HQP suggest to modify the summary of changes.

The word “Managed” should be in lower case for paragraph in the page 56 of 62 “**Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity”**.

It could be usefull to introduce base of risk in the case of a TCA connected to LOW impact BES systems without external connectivity.

Likes 0	
Dislikes 0	
Response	

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	Yes
Document Name	
Comment	
Santee Cooper agrees with APPA's comments.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Recommend revisions to remove the bulleted list and re-write the requirements. The bullet points should go into the GTB section so that there is less chance for a misinterpretation that would require the implementation of more than one of the bulleted point in order to meet compliance.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobby Olsen - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
Ryan Olson - Portland General Electric Co. - 5

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
We continue to have concerns about how the GTB are factored into Compliance and Enforcement. In some cases it appears that they create “requirements” that must be incorporated into your program; this is inconsistent with prior FERC precedent. On the other hand, it is not clear whether or not you can rely on the GTB in developing your program and ensuring compliance. This concern continues to fail to be addressed by the SDT. With respect to Attachment 1 Section 3, and Attachment 2, Section 3.1, it doesn't make sense to keep referring to physical location when it comes to electronic controls (as previously noted).	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	
Document Name	
Comment	
Yes	
Likes 0	
Dislikes 0	
Response	

4. Attachment 2: The SDT revised the evidential language of CIP-003-7(i), Attachment 2, Section 5 to make the Measures consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

The complexity of the sentences are difficult to read and understand. Suggest revising to bulleted lists. The evidence requirements seem to require an inventory of TCA's and RM. This could be an issue in the same way that a list of BES Cyber Systems has been determined to be an issue.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Reclamation appreciates the Standards Drafting Team's consideration of prior recommendations. Reclamation agrees with the changes and has the following question:

In this version of CIP-003-7(i), did the SDT intend to add guidance regarding the new section on page 9 under Requirement 1 "1.2.6 Declaring and responding to CIP Exceptional Circumstances" in Attachment 1 and/or Attachment 2?

Likes 0	
Dislikes 0	

Response

Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators

Answer	No
Document Name	

Comment
We disagree with the proposed language, as the SDT has only restated the content of the requirement language. There is no process or guidance for an entity to follow when a vendor fails to comply with required request. Is a vendor's attestation sufficent proof for an entity to demonstrate reasonable assurance for compliance? If so, an attestation should be included in the list of acceptable evidence for this requirement, and reflected in Attachment 2 to ensure consistent regional application.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	

Comment
This change creates additional requirements for Low Impact BCS relating to change control (additional cost implications from an administrative standpoint with limited reliability benefit) (i.e. capture every time a TCA is connected to a system and this infers that an entity is required to document a discrete list of Cyber Assets for Low Impact BCS) NRG recommends deleting the quoted portion of the phrase from Section 5 of Attachment 2, number 2: Examples of evidence for Section 5.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures "that document a review of the installed antivirus update level" because it imposes change management requirements where there are not existing NERC requirements

Likes 0	
Dislikes 0	

Response

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	No
Document Name	

Comment
ITC Holdings agrees with the comment submitted by NSRF – see below: Please see question 3 for comments concerning "review". By explaining what the acceptable level of "review" is, the small entity will not be caught in a catch 22. Whereby the "other party" will not state that they meet the attributes of 5.2 and the small entity will have a Low Impact BES Cyber System that cannot be upgraded.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

Considering the current draft language of the standard, the required evidence can be improved. There is a tradeoff that must be considered between adequate evidence to demonstrate both 1) compliance and assurance that the risk of introduction of malware is mitigated and 2) evidence collection across a large number of sites becoming excessively burdensome. The standard and evidence must be both effective and efficient.

The expectations for adequate evidence do not fit the audit style currently being used in compliance monitoring. For example, the CIP Version 5 Evidence Request is clearly written to require often extensive documentation of implementation, whereas the measures documented are inconsistent. The measures should be built to provide an example of evidence that would either meet the current evidence request approach or to clearly communicate the intent of the SDT what appropriate evidence would be.

For Measure 5.1, an example of alternative language to clarify audit expectations would be:

Examples of evidence for Section 5.1 may include, but are not limited to,

1. **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; and**

2. **Either documentation of an appropriate set of controls that provide a high level of assurance that malware is not present on the Transient Cyber Asset prior to use; or documentation that the Transient Cyber Asset followed the documented method and demonstrates that no identifiable malware is present prior to use.**

If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

For Measure 5.3, an example of alternative language that may meet this intent could include:

Examples of evidence for Section 5.3 may include, but are not limited to,

1. **Documented process(es) of the method(s) used to detect malicious code; and**

2. **Either documentation of an appropriate set of controls that provide a high level of assurance that malware is not present on the Removable Media prior to use; or documentation that the Transient Cyber Asset followed the documented method and demonstrates that no identifiable malware is present prior to use.**

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	No
Document Name	
Comment	
We recommend modifying the first sentence of 5.3.1 to read: “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, including an example of the results.” The original language is confusing, and we believe we should avoid the suggestion of a requirement to capture and retain transactional-level evidence as this would be administratively burdensome.	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6	
Answer	No
Document Name	
Comment	
CIP-003-7(i), Attachment 2, Section 5, Part 3 is inconsistent with Part 1. Part 3 states that “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”. Entergy views the documented process(es) and the results of scanning as two separate pieces of evidence. Part 1 identifies the documented process(es) as an acceptable form of evidence with no requirement for scan results for TCA. Part 3 as written implies that all scans results of applicable Removable Media must be maintained in order to provide proper evidence of compliance with CIP-003-7(i), Attachment 1, Section 5.3. This is in stark contrast to the proposed “Supplemental Material” which states that “the SDT does not intend for a Responsible Entity to conduct a review for every single connection of that Removable Media, but implement their process(es) in manner that protects all BES Cyber Systems where the Removable Media may be used. The intent is also not to require a log documenting each connection of Removable Media to a BES Cyber Asset.” Entergy proposes that CIP-003-7(i), Attachment 2, Section 5, Part 3 be rewritten to more closely mirror Part 1 which identifies the documented process as the evidence item. Specific scan results should be identified as potential additional evidence to support Registered Entities programs.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	

Seattle City Light agrees with the revisions so far as they go, but finds that they do not address the question of what would be acceptable evidence of the existence of any Low impact Removable Media Asset (based on the proposed definition) in the absence of an explicit list of Low impact BES Cyber Systems and Assets at a facility. As discussed in the definition comment above, Seattle does not have a solution to the problem, which is inherent to the structure of CIP verion 5/6.

Likes 0	
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

Same as previous answer.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5

Answer	No
Document Name	

Comment

We continue to have concerns about how the GTB are factored into Compliance and Enforcement. In some cases it appears that they create “requirements” that must be incorporated into your program; this is inconsistent with prior FERC precedent. On the other hand, it is not clear whether or not you can rely on the GTB in developing your program and ensuring compliance. This concern continues to fail to be addressed by the SDT. With respect to Attachment 1 Section 3, and Attachment 2, Section 3.1, it doesn't make sense to keep referring to physical location when it comes to electronic controls (as previously noted).

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No

Document Name	
Comment	
Please see question 3 for comments concerning “review”. By explaining what the acceptable level of “review” is, the small entity will not be caught in a catch 22. Whereby the “other party” will not state that they meet the attributes of 5.2 and the small entity will have a Low Impact BES Cyber System that cannot be upgraded.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	

There is a concern with the requirement that not only requires an inventory of Transient Cyber Assets and Removable Media but it also requires evidence of chain of custody. The SDT needs to provide clarity on what is required for "evidence of chain of custody".

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	Yes
Document Name	

Comment

Section 5.1 in page 32 to 62: To lighten a obligation of maintaining an inventory of TCA of *Low impact BES Cyber System,* HQP suggest to remove the notion of Trancient asset capability and change the paragraph by " the Responsible Entity or the vendor may document the method used to mitigate the introduction of malicious code"

Likes 0	
Dislikes 0	

Response

Roger Dufresne - Hydro-Qu?bec Production - 5

Answer	Yes
Document Name	

Comment

Section 5.1 in page 32 to 62: To lighten a obligation of maintaining an inventory of TCA of *Low impact BES Cyber System,* HQP suggest to remove the notion of Trancient asset capability and change the paragraph by " the Responsible Entity or the vendor may document the method used to mitigate the introduction of malicious code"

Likes 0	
Dislikes 0	

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer	Yes
Document Name	

Comment	
Tacoma Power supports comments submitted by APPA. Does the Standards Drafting Team intend that any kind of sign-in sheets may be required at assets containing low impact BES Cyber Systems?	
Likes 0	
Dislikes 0	
Response	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
The complexity of the sentences are difficult to read and understand. Suggest revising to bulleted lists. The evidence requirements seem to require an inventory of TCA's and RM. This could be an issue in the same way that a list of BES Cyber Systems has been determined to be an issue.	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobby Olsen - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE noticed the following:

- Page 31, Section 1. Cyber Security Awareness; there is an extra “_” that is not needed after the colon symbol.
- Page 31, Section 2. Physical Security Controls; there is an extra “_” that is not needed after the colon symbol.
- Page 33, Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation; there no period ”.” at the end of the first continued paragraph.

Likes 0	
Dislikes 0	
Response	

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides examples of temporarily connected devices, and strategies to consider in developing the Transient Cyber Asset and Removable Media malicious code mitigation plan(s) at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	No
Document Name	
Comment	
We continue to have concerns about how the GTB are factored into Compliance and Enforcement. In some cases it appears that they create “requirements” that must be incorporated into your program; this is inconsistent with prior FERC precedent. On the other hand, it is not clear whether or not you can rely on the GTB in developing your program and ensuring compliance. This concern continues to fail to be addressed by the SDT. With respect to Attachment 1 Section 3, and Attachment 2, Section 3.1, it doesn't make sense to keep referring to physical location when it comes to electronic controls (as previously noted).	
Likes 0	
Dislikes 0	
Response	

Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Same as previous answer	
Likes 0	
Dislikes 0	
Response	

Julie Hall - Entergy - 6	
Answer	No
Document Name	
Comment	

Supplemental Material, Requirement R2, Attachment 1, Section 5.1 – Transient Cyber Asset(s) Managed by the Responsible Entity, Paragraph 4 states that if a device will be used to “For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.” This may imply that at least *some* logs might need to be created for connections of TCA to BCA, which is not a requirement stated in the standard for TCAs at low impact BCS, or even for TCAs at Highs and Mediums under CIP-010-2. Additionally, requiring documentation that a TCA was updated before connecting to a BCA removes the device from the on-going program and puts it into on-demand space due to “has been updated before being connected” implying the device is as up to date as possible, even though the on-going process may allow for devices to be updated on a longer regular interval. If the TCA was truly maintained as part of the entitiy’s on-going program, no additional log or documentation should be required as the device would be compliant with the standard as written.

Supplemental Material, Requirement R2, Attachment 1, Section 5.1 – Transient Cyber Asset(s) Managed by the Responsible Entity, Paragraph 4Mitigation of the threat of detected malicious code on the Removable

Media prior to connecting Removable Media to a low impact BES Cyber System.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA believes that for Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems--entities must manage these assets under the program that matches the highest impact level to which they will connect.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

Considering the current draft language of the standard, the GTB addresses the required points. However, the messages are not clearly, simply, and constructively communicated. While the teams have clearly put a considerable amount of work into ensuring each detail is

correct, the overall message in the guidance gets lost. This results in opportunities for multiple different interpretations by various entities and auditors.

One possible control is testing the operation of antivirus to test signatures. These should be specifically noted that use of test signatures is not considered identified malware.

Section 5.2 (and likely all of the guidance) could be improved if the GTB approach was changed to treat malware protection as a program with specific objectives and a selection of example techniques that may be used to meet these objectives. Further, the guidance should be coordinated with the requirements in development by the Supply Chain SDT.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns

Answer	No
Document Name	

Comment

ITC does not agree with the proposed modification in regards to guidance provided for awareness training. The revised guidance states "The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel". This statement is ambiguous and leaves the interpretation as to whether or not tracking of reception of awareness training is actually required to maintain compliance. The specific and direct language of "Responsible Entity is not required" should be retained, to reduce confusion and ambiguity as to if this is required for compliance and not left to the disposition of individual auditors. ITC recommends that this specific change be struck and the original language to stand.

All other changes are acceptable.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG recommends correction of grammatical / spelling error: on page 57 of 62 of the Guidelines and Technical basis section for requirement 2.

• If a Responsible Entity chooses *to use* methods that mitigate the introduction of malicious code other than those listed, it should *document* ***at*** how the other method(s) meet the mitigation of the introduction of malicious code objective.

Pertaining to project 2016-02, NRG recommends that the Low Impact requirements should be incorporated into the existing CIP standards using applicability tables because this would remove inconsistencies and confusion between L/M/H and provide more efficiency within the industry. For example, applied CIP-010-2 Attachment 1 for TCA and Removable Media requirements, with the exception of the authorized user or machine lists.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Reclamation appreciates the Standards Drafting Team's consideration of prior recommendations. Reclamation agrees with the changes and has the following comment:

In the redline version of the Guidelines and Technical Basis, some typographical errors include:

- The spelling of "Responsible Entities" on the sixth line of page 55.
- A duplicate paragraph at the bottom of page 56 and the top of page 57.
- The spelling of "to use" and "document" in the third bullet of page 57.
- The word "is" at the beginning of a sentence on the third line from the bottom of page 57.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The information in the GTB section does not appear to be consistent with the information in Requirement R2. Our interpretation of Requirement R2 suggests that there is not enough clarity in the Requirement to differentiate whether the focus is solely on CIP-002 and its attachment 1 or is the focus more on CIP-003-7(i) and its Attachment 1. We suggest adding clarity to the Requirement and/or the GTB to ensure that there is no confusion as to the Requirement's intent as well as what an audit team's interpretation of the performance of an entity during the auditing process.

Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes. To avoid confusion with CIP-010 R1 requirements, we suggest the removal of "change management process" in the prior sentence.	
Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

Seattle City Light appreciates the extra efforts of the Standard Drafting Team to provide such guidance and technical information. However, Seattle asks that Guidelines and Technical Basis information be provided for new Section 1.2.6 as well. This guidance would address how a CIP Exceptional Circumstance is considered when applied against a requirement that does not explicitly mention that a CIP Expection Circumstance applies.

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities

Answer	Yes
Document Name	

Comment

1) The guidance should be coordinated with the Supply Chain SDT.

2) The GTB language that states: “Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.” is to prescriptive. Recommend that the “are to” be changed to “may”. The use of prescriptive language like “should” and “are to” should be used on a very limited basis if not removed entirely. Guidance should be shifted to a programmatic approach.

Likes 0	
Dislikes 0	

Response

Bob Thomas - Illinois Municipal Electric Agency - 4

Answer	Yes
Document Name	

Comment

Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.

Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Page 56 of the Guidelines and Technical Basis includes a section titled “Vulnerability Mitigation”; however, Requirement R2, Attachment 1, Section 5 is titled “…Risk Mitigation”. AZPS requests clarification and consistency regarding the terms vulnerability and risk as one term is more subjective than the other.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
No comments for section 5.	

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG

Answer	Yes
Document Name	

Comment

Two comments.

First, recommend changing “should” to “may” in this paragraph

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.1 Procurement language may unify the other party’s and entity’s actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party’s support. Entities should consider the “General Cybersecurity Procurement Language” and “The Supplier’s Life Cycle Security Program” when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Second, recommend updating 5.3 from “If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System.“ to “If malicious code is discovered, it must be removed or mitigated prior to connection to a BES Cyber Asset or BES Cyber Systems in order to prevent the malicious code from being introduced into the BES Cyber Asset or BES Cyber System.“

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
The guidance should be coordinated with the Supply Chain SDT.	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobby Olsen - Salt River Project - 6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE noticed the following:

- Page 56, Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity states, "*For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect*." Since this concept is the same as described in the Guidelines and Technical Basis of CIP-005-5, Texas Re suggests that the SDT use the same "high water mark" language found in the Guidelines and Technical basis of CIP-005-5 to stay consistent.

- Page 57, Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity states, "*The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset*." Texas RE considers keeping a list of BES Cyber Assets as best practice and this language discourages it. Texas RE encourages entities to have an inventory of their low impact BES Cyber Systems.

- Page 57, Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity states, "*If a Responsible Entity chooses touse methods…*." There should be a space between "touse".

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	
Document Name	

Comment

1) The guidance should be coordinated with the Supply Chain SDT.

2) The GTB language that states: "Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed." is to prescriptive. Recommend that the "are to" be changed to "may". The use of prescriptive language like "should" and "are to" should be used on a very limited basis if not removed entirely. Guidance should be shifted to a programmatic approach.

Likes 0	
Dislikes 0	

Response

6. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

We suggest the drafting team include the approval of the RSAW into the Implementation Plan as this is a significant and related document.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

Pertaining to project 2016-02, CIP-003-7(i), it doesn't appear that the implementation plan accounts for additional time to implement 1.2.5 and 1.2.6. NRG recommends that the implementation plan allow for 18 months implementation time of 1.2.5 and 1.2.6. (the same implementation time as other requirements)

Likes 0	
Dislikes 0	

Response

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns

Answer	No
Document Name	

Comment

ITC Holdings agrees with the comments compiled by the EEI CIP Standards subgroup– see below:

SUMMARY:

CIP-003-6, Requirement R2, Attachment 1, sections 2 and 3 have been approved (under the Order No. 822 implementation plan) to be effective on September 1, 2018. However, in Order No. 822, the Commission ordered NERC (within 1 year) to provide clarity regarding the LERC (Low Impact External Routable Connectivity) definition, specifically ambiguity surrounding the term "direct" used in the definition. When the SDT set out to modify the definition they found that it was more appropriate to modify the requirement language to address the ambiguity. The modified standard (version 7) is expected to be filed with FERC by March 31, 2017.

CIP-003-6, Requirement R2, Attachment 1, sections 2 and 3 is effective September 1, 2018 and version 7, if FERC approves, will be effective 18 months from FERC's approval, so doing rough math (March 31, 2017 NERC filing of version 7, August 2017 NOPR--assuming ~5 months FERC review, February 2018 FERC approval--assuming 60 day notice and comment, and 3 month FERC review): version 7 would become effective around August 2019, basically a year after Version 6 (the time it took NERC to make the modification).

RATIONALE:

Reasons for supporting a change to the implementation plan: 1) retiring the implementation of CIP-003-6, attachment 1, sections 2 and 3; 2) synching up the implementation the low impact BES Cyber System modifications (attachment 1, sections 2, 3, and 5); and 3) giving entities 18 months to implement these sections:

1. Companies will not have certainty regarding CIP-003-6 implementation until February 2018, but will have to move forward on version 6 to make the Sept. 2018 compliance deadline or accept the compliance risk by not implementing version 6.

2. According to the Commission (Order No. 822), the CIP-003-6 modification "is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition." As a result, implementation of CIP-003-6 without the modification doesn't make much sense in light of the ambiguity identified by the Commission.

3. Low impact BES Cyber Systems (LIBCS) have a low impact to the BES compared to medium and high impact BES Cyber Systems.

4. LIBICS number in the tens of thousands systems; it will take time to carefully implement the new CIP-003 requirements. Implementing CIP-003-6 LERC, CIP-003-7 LERC, and then CIP-003-7 TCA in three steps will strain resources for systems with low impact to the BES. It would be more efficient to implement just the CIP-003-7 LERC and TCA modifications at the same time.

5. Change management at this scale, will also be more effective if done all at once, which will help reduce the potential spike in audit violations.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

While achievable in 18 calendar months, the standard needs significant improvement before a yes vote on the implementation.

Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6	
Answer	No
Document Name	
Comment	
Entergy cannot agree with the Implementation Plan timeline given the standard as written, and the concerns discussed in the comments submitted above. Until clarity is given regarding the scope and evidentiary requirements necessary to achieve compliance, Entergy cannot support the short implementation timeline proposed as the feasibility of implementing controls and evidenciary requirements to meet the standard as currently drafted in that small timeframe for an Entity as large as Entergy is miniscule.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
The majority of actions necessitating the timeframe proposed in the Implementation Plan modifications involve identifying and implementing the physical, electronic, and TCA/RM controls necessary for over 1200 assets containing Low Impact BES Cyber Systems, as well as training a massive amount of personnel on meeting and maintaining compliance with these new Standard requirements. Although the requirements themselves may be less rigid than those for Highs and Mediums, the proposed implementation timeframe is required from a volume standpoint, as well as from a risk-based standpoint so as not to divert attention and resources away from meeting and maintaining compliance on all of the other High and Medium risk assets	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
We strongly support the Implementation Plan, which seeks to replace compliance with CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 with compliance with CIP-003-7(i) (and CIP-003-7) such that only one implementation is required for the LIBICS modifications, 18 months from FERC approval. Our members agree with the SDT's approach and offer further explanations as to the importance of this implementation plan:	

1. For CIP-003 alone, EEI members are looking at 3 implementation phases for a very large group of disaggregate assets (substations with variations among systems, types, shared footprints and components as well as generating stations that are extremely complex with many different systems and manufacturers involved). LIBCS number in the tens of thousands of systems; it will take time to carefully implement the new CIP-003 requirements. Implementing CIP-003-6 LERC, CIP-003-7 LERC, and then CIP-003-7 TCA in three steps will strain resources for systems with low impact to the BES.

2. Change management at this scale, will also be more effective if done all at once, which will help reduce the potential spike in audit violations. When we say more effective, we really mean doing it right for security and reliability. Training on one change for CIP-003-6 and then training again for CIP-003-7 will create confusion for field forces. Having one date to train on this culture change management would be more effective when an entity needs to train 250 plus field and engineering people regarding 550 or more low impact BES Cyber Systems. If field people are confused, they will make or may be prone to make mistakes due to confusion or rapidly changing expectations. Potential violations will not protect against security threats or reliability issues.

3. Shared facilities create another implementation issue. For example, an EEI member has approximately half of their low impact substations owned by third parties, shared facilities. To make each of the section 2 and 3 changes, they will have to physically go to each substation, which are owned by different entities and as a result are all different. As a result, the approaches they take at each facility must be different, which is also a good thing in the security world. Eighteen months is necessary to make these changes.

4. The revised CIP-003-7 language including retirement of the LERC definition improves the clarity of the requirements. However, the revisions represent a change in assessment approach and will precipitate a new analysis of which locations will be in scope for section 3. The LERC definition provided a filter by the use of the word 'direct' that could be applied when determining which locations were in scope. The retirement of LERC removed that filter. The new language replacing the LERC definition established new assessment criteria and applies it regardless of direct or indirect connectivity. The change to LERC requires Responsible Entities to perform a new analysis of each of their locations. Applying the CIP-003-7 requirements means that entities must walk down each location in scope to determine the specific configurations (physical and electronic) that exist at the location. These walk downs are currently underway to apply a -6 implementation focused on the definition of LERC from CIP-003-6. The scope of analysis will change under CIP-003-7, so that all locations must be assessed for connectivity and then assessed against the new criteria.

Likes 0	
Dislikes 0	

Response

Roger Dufresne - Hydro-Qu?bec Production - 5

Answer	Yes
Document Name	

Comment

No comments for section 6.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy agrees with EEI's comments regarding the implementation plan for the Low Impact BES Cyber System modifications.	
Likes 0	
Dislikes 0	
Response	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the comments submitted by EEI regarding the proposed Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	Yes

Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Companies with a large number of low impact assets will need this time to educate users about handling TCAs and Removable Media. These assets are categorized as low impact because they inherently have a low ability to negatively impact the Bulk Electric System. We do not want to focus our resources on rolling out this education at the expense of efforts that mitigate risks to assets that inherently have a greater ability to negatively impact the Bulk Electric System. During the 18-month implementation plan, we will design the overall processes taking into consideration differences between different plant types (gas, lignite, combustion turbine and combined cycle). We will roll out that program to a single pilot plant to identify lessons learned and improve the experience as we onboard subsequent plants. We anticipate spending 3-5 months to design the processes and pilot the program. The remaining months will be spent rolling out to our fleet (40 units at 15 plants). The 18-month implementation plan is appropriate as it allows us to carefully and thoughtfully assign resources to most effectively and efficiently mitigate cyber risk.	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobby Olsen - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not necessarily object to the SDT's proposed 12-month implementation period. However, Texas RE respectfully requests that the SDT provide a basis for its decision to adopt such a 12-month compliance window, including any data it considered in determining that this was an appropriate window for affected entities to meet their compliance obligations under the revised Standards.	
Likes 0	
Dislikes 0	
Response	

7. If you have additional comments on the proposed revisions to address the FERC directive regarding TCAs for low impact BES Cyber Systems that you have not provided in response to the questions above, please provide them here.

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	
Document Name	

Comment

Small entities will not be able to go up against a vendor (i. e. Micro Soft in size) and request to review their most current protections to comply with section 5.2. The above clarity will assure we meet the attributes of 5.2. The NSRF does not wish for CIP-003-7(i) to be the number one non compliance Standard going forward in NERC, similar to CIP-007-6.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	
Document Name	

Comment

Entities are increasing their use of malicious code mitigation using tools such as Cylance, which does not rely on signatures or updates. The measures should consider these tools and provide examples of evidence that will prove compliance.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5

Answer	
Document Name	

Comment

none

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	
Document Name	

Comment

Dominion recommends that the first VSL conditional statement for Requirement 1 Part 1.2 (page 14 of 62 of draft 1 of CIP-003-7(i)) be consistent with the prior version of CIP-003 and read as follows:

Lower VSL: The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two or fewer of the six topics required by R1. (R1.2)

Moderate VSL: The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the six topics required by R1. (R1.2)

High VSL: The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four of the six topics required by R1. (R1.2)

Severe VSL: The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address five or more of the six topics required by R1. (R1.2)

The revised VSLs accurately reflect the actual severity when a failure to address the appropriate topics occurs.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC

Answer	
Document Name	

Comment

Seattle City Light has additional concerns that led it to vote NO for this ballot. One concern is about new sub-part 1.2.6, which introduces CIP Expectional Circumstances to Low impact facilities. The other concern is about seeming errors in the Violation Severity Level (VSL) tables for some of the new parts and sections introduced in CIP-003-7(i).

Regarding sub-part 1.2.6, Seattle supports the concept of allowing CIP Exception Circumstances for Low impact facilities and related requirements, and find this idea highly sensible and reasonable. Seattle is concerned, however, that the change appeared without notice or discussion in the present draft of CIP-003-7(i), and that the application of CIP Expectional Circumstances for Lows is not at all defined. In particular, other Standards, parts, and sub-parts of CIP version 5/6 explicitly identify where CIP Exceptional Circumstances are allowed. This explicit mention creates the presumption that CIP Exceptional Circumstances are allowed only for said Standards, parts, or sub-parts; some auditors have stated as such. Seattle is aware that an drafting team effort is planned to address inconsistencies in the existing application of CIP Exceptional Circumstances, and finds it premature to expand the use of CIP Exceptional Circumstances in a way that introduces even more uncertainty—how are they applied to Lows where no existing Low Standard mentions that CIP Expectional Circumstances are allowed—before the existing issues are addressed. That the concept was introduced without discussion or technical guidance language only heightens our concern. As a possible corrective, Seattle recommends that the Part R2 of CIP-003-7(i) be modified as follows (BOLD text is new):

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall, EXCEPT FOR CIP EXCEPTIONAL CIRCUMSTANCES, implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.

Regarding the VSL tables, Seattle does not understand the difference among the Lower, Moderate, and High VSLs for failure to perform some or all of the activities according for Requirement R2, Attachment 1, Section 5.1. For Transient Cyber Assets, the Lower VSL states:

The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2)

The applicable Moderate VSL states:

The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2)

And the applicable High VSL reads:

The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2)

Seattle does not understand the difference among the three items, given that the failure to manage according to plan (the Lower VSL) means that introduction of mitigation code is not documented (the Moderate VSL) and/or mitigated (High VSL); there are not other applicable activities to fail. As such, Seattle recommends these be consolidated into a single VSL at the Moderate (or perhaps High) level.

Finally, Seattle also finds confusing the wording in the Lower VSL for Removable Media. For Transient Cyber Assets this VSL states:

The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)

Seattle does not understand how an entity can ever meet the Lower VSL for Removable Media, in that to do so it must “document its plan(s) for…Removable Media but fail to document the Removable Media section(s) according to Requirement 2.” As best as we understand, the Removable

Media Plans are the Removable Media sections of Requirement 2, so the statement appears to be in error. As a corrective, Seattle suggests that the Lower VSL entry for Removable Media be modified to mirror that of Transient Cyber Assets, and thus read (BOLD indicates where “Removable Media” was substituted for Transient Cyber Asset):

The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its REMOVABLE MEDIA according to Requirement R2, Attachment 1, Section 5.1. (R2)

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

BPA respectfully suggests spellchecking the redline before finalizing. For example:

Page 33: Entiteis

Page 57: Transiet

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities

Answer	
Document Name	
Comment	
1) The word “and” should be added at the end of R1.2.5 2) This comment form did not reference the addition of CIP Exceptional Circumstances as Requirement R1.2.6 and the inclusion of the phrase “except under CIP Exceptional Circumstances” in Attachment 1, Section 5. The “except under CIP Exceptional Circumstances” phrase should also be addressed in Attachment 1 Sections 2 and 3. Not addressing CEC in Sections 2 and 3 may result in a “no” vote for on future ballot of this standard. 3) A Section 6 under Attachment 2 is needed to explain how the CIP Exceptional Circumstance is to be used so you can put it into your policy/plan accordingly.	
Likes 0	
Dislikes 0	
Response	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	
Document Name	
Comment	
none	
Likes 0	
Dislikes 0	

Response
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5
Answer	
Document Name	
Comment
no
Likes 0	
Dislikes 0	
Response
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5
Answer	
Document Name	
Comment
none
Likes 0	
Dislikes 0	
Response
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns
Answer	
Document Name	
Comment
ITC Holdings agrees with the comment submitted by NSRF – see below: Small entities will not be able to go up against a vendor (i. e. Micro Soft in size) and request to review their most current protections to comply with section 5.2. The above clarity will assure we meet the attributes of 5.2. The NSRF does not wish for CIP-003-7(i) to be the number one non compliance Standard going forward in NERC, similar to CIP-007-6.
Likes 0	

Dislikes 0	
Response	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	
Document Name	
Comment	
none	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5	
Answer	
Document Name	
Comment	
no	
Likes 0	
Dislikes 0	
Response	
Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	
Document Name	
Comment	
1. The inclusion of CIP Exceptional Circumstance for lows adds additional compliance burden above and beyond the FERC Directives. This will require Cyber Security Policy revisions, training and increase audit risk for lows who have not seen any addtioal risks to the BES to require CIP Exceptional Circumstances as part of their CIP cyber Security Program. 2. If a low impact entity connects an identified 30-day TCA beyond the thirty days, what is the classification of the asset? If this was a high or medium impact entity, the TCA would be classified as a Protected Cyber Asset (PCA). However, PCAs are not applicable to low impact entities, as a low impact's TCA would not be classified as a BES Cyber Asset that could impact the BES within 15 minutes. Would the low impact entity who failed to connect the TCA within the thirty day timeframe have to self-report the TCA to Regional Entities? If so, this would impose a greater violation risk for lows than for high and medium impact entities. 3. We thank the SDT for this opportunity to provide comments.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	

Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
No comments for section 7.	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	
Document Name	
Comment	
Some typos: P 55: 'entiteis' P 70 of 75: “touse”; “. is the SDT”; “toTransiet Cyber Assets”	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	
Document Name	
Comment	
Xcel Energy supports the comments of the Edison Electric Institute.	

Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	
Document Name	
Comment	
The CIP Exceptional Circumstance concept does not belong with the Low Impact requirements. The purpose of CIP-007-3i was to define and create requirements for Transient Cyber Assets and Removable Media. The need for Exceptional Circumstances for High and Medium is because the Standard mandates a PRA for unescorted access. Even with Exceptional Circumstances you have to report a violation because of the externally mandated PRA. In the case of Low Impact, the entity writes the requirements for access. Most departments responsible for physical security automatically allow the entrance of Emergency Personnel and Police if there is an alarm or 911 call. This could be written into each Responsible Entity's Low Impact Cyber Security Policy (CIP-003 R1.2) but that doesn't seem to support BES Reliability.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE notes some possible issues with the proposed Violation Severity Levels associated with the proposed additions to CIP-003, Attachment 1. First, the second proposed “Lower VSL” provides that “[t]he Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to Requirement R2, Attachment 1, Section 5.3.” Although it is possible to read the VSL language as referring first to general documentation for TCAs and Removable Media and then to the two specific Removable Media elements identified in Section 5.3, this connection could be made clearer. One approach would be revise the Lower VSL to read “The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the use of method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or mitigation of the threat of detected malicious code on Removable Media prior to connecting Removable Media to a low impact BES Cyber System.” Second, and related to the first issue above, the initial additional “Moderate VSL” provides that the Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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.” (emphasis added). However, Section 5.3 applies to Removable Media and not TCAs. As such, the reference here seems inappropriate and potentially conflicts with the “Low VSL” for documentation of Removable Media mitigation described above. Texas RE recommends that the SDT either eliminate the reference to Section 5.3	

here, or develop a new “Moderate VSL” applicable to the mitigation requirements for Removable Media in Section 5.3. The Standard Drafting Team should further ensure that this approach is consistent with the “Low VSL” for Removable Media documentation as well.

Finally, while Texas RE does not necessarily object to the general VSL assignments at this time, Texas RE respectfully requests that the SDT provide a basis for its decisions to assign VSL categories to the various elements. In particular, Texas RE would like to understand the SDT’s decision to assign “Low” and “Moderate” VSL categories to Removable Media and “Moderate” and “High” VSL categories to Transient Cyber Assets.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	
Document Name	

Comment

1) The word “and” should be added at the end of R1.2.5

2) This comment form did not reference the addition of CIP Exceptional Circumstances as Requirement R1.2.6 and the inclusion of the phrase “except under CIP Exceptional Circumstances” in Attachment 1, Section 5. The “except under CIP Exceptional Circumstances” phrase should also be addressed in Attachment 1 Sections 2 and 3. Not addressing CEC in Sections 2 and 3 may result in a “no” vote for on future ballot of this standard.

3) A Section 6 under Attachment 2 is needed to explain how the CIP Exceptional Circumstance is to be used so you can put it into your policy/plan accordingly.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	
Document Name	
Comment	
To address the changes to the RSAW provided on January 20th Under the Note to Auditor section, Attachment 1, Section 3: Bullet 1: Recommended to state that “the devices used to control electronic access” can be documented at a representative level. The standard (Attachment 1, Section 3, Bullet 1) under examples of evidence state that documentation can be “at each asset or group of assets containing low impact BES Cyber Systems” level and can be representative diagrams, meaning a list of devices at each asset is not required under the standard and puts additional documentation burden on the Entity as currently worded in the RSAW. Bullet 2: Recommended to document necessary inbound and outbound routable protocols communications at a standard level versus at each asset (e.g. document SCADA communications as necessary inbound and outbound for the Entities entire system, rather than having to document at each asset) for same reason as our comment for Bullet 1. Bullet 3 and 4: Recommended to document that the electronic access controls can be provided at a standard level (e.g. standard configurations) which would apply to the standard devices, versus providing per asset.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	
PacifiCorp supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	

Answer	
Document Name	
Comment	
1) This comment form did not reference the addition of CIP Exceptional Circumstances as Requirement R1.2.6 and the inclusion of the phrase “except under CIP Exceptional Circumstances” in Attachment 1, Section 5. The “except under CIP Exceptional Circumstances” phrase should also be addressed in Attachment 1 Sections 2 and 3.	
Likes 0	
Dislikes 0	
Response	

Additional comments received from American Public Power Association

1. Definition: The SDT revised the definition of Transient Cyber Asset such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes: X

   No:

   Comments: Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP’s and PCA’s to the Transient Cyber Asset definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.

2. Definition: The SDT revised the definition of Removable Media such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes: X

   No:

   Comments: Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP’s and PCA’s to the Removable Media definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.

3. Requirement R2: The SDT revised CIP-003-7(i), Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to mitigate the risk of propagation of malware from transient devices. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes: X

   No:

   Comments: 1) The bulleted list creates requirements that are too prescriptive. Use alternative language for Section 5.1 and 5.2 to remove the bullet points (because they may be used against you in some fashion in the future), and re-write the requirements. The bullet points should go into the GTB section so that there is less chance for a misinterpretation or reinterpretation that would require the implementation of more than one of the bulleted point in order to meet compliance.

   2) As written, the requirements listed for TCAs in CIP-003-7(i) for Low Impact assets is a subset of the requirements for high and medium impact included in CIP-010-2 R4. If this list remains the same or if changed the GTB section should include a statement that low impact requirements are a subset of those for High and Medium.

4. Attachment 2: The SDT revised the evidential language of CIP-003-7(i), Attachment 2, Section 5 to make the Measures consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes: X

   No:

   Comments: The complexity of the sentences are difficult to read and understand. Suggest revising to bulleted lists. The evidence requirements seem to require an inventory of TCA's and Removable Media. This could be a significant burdent on registered entities in the same way that a list of BES Cyber Systems has been determined to be an issue.

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides examples of temporarily connected devices, and strategies to consider in developing the Transient Cyber Asset and Removable Media malicious code mitigation plan(s) at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

   Yes: X

   No:

   Comments: 1) The guidance should be coordinated with the Supply Chain SDT.

   2) The GTB language that states: "Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed." is too prescriptive. Recommend that the "are to" be

changed to “may”. The use of prescriptive language like “should” and “are to” should be used on a very limited basis if not removed entirely. Guidance should be shifted to a programmatic approach.

6. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority’s order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

   Yes: X

   No:

   Comments: None

7. If you have additional comments on the proposed revisions to address the FERC directive regarding TCAs for low impact BES Cyber Systems that you have **not** provided in response to the questions above, please provide them here.

   Comments: 1) The word “and” should be added at the end of R1.2.5

   2) This comment form did not reference the addition of CIP Exceptional Circumstances in Requirement R1.2.6 and the inclusion of the phrase “except under CIP Exceptional Circumstances” in Attachment 1, Section 5. The “except under CIP Exceptional Circumstances” phrase should also be addressed in Attachment 1 Sections 2 and 3. Not addressing CIP Exceptional Circumstances in Sections 2 and 3 may result in a “no” vote on future ballot of this standard.

   3) A Section 6 under Attachment 2 is needed to explain how the CIP Exceptional Circumstance is to be used so you can put it into your policy/plan accordingly.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2016-02 Modifications to CIP Standards | CIP-003-7(i), Implementation Plan, and definitions of TCA and Removable Media
Comment Period Start Date:	12/12/2016
Comment Period End Date:	1/25/2017
Associated Ballots:	2016-02 Modifications to CIP Standards CIP-003-7(i) Implementation Plan IN 1 OT 2016-02 Modifications to CIP Standards CIP-003-7(i) IN 1 ST 2016-02 Modifications to CIP Standards Removable Media | New Definition IN 1 DEF 2016-02 Modifications to CIP Standards Transient Cyber Asset | New Definition IN 1 DEF

There were 50 sets of responses, including comments from approximately 136 different people from approximately 110 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Director of Standards Development, Steve Noess (via email) or at (404) 446-9691.

Questions

1. Definition: The SDT revised the definition of Transient Cyber Asset such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

2. Definition: The SDT revised the definition of Removable Media such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

3. Requirement R2: The SDT revised CIP-003-7(i), Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to mitigate the risk of propagation of malware from transient devices. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

4. Attachment 2: The SDT revised the evidential language of CIP-003-7(i), Attachment 2, Section 5 to make the Measures consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides examples of temporarily connected devices, and strategies to consider in developing the Transient Cyber Asset and Removable Media malicious code mitigation plan(s) at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

Questions

6. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

7. If you have additional comments on the proposed revisions to address the FERC directive regarding TCAs for low impact BES Cyber Systems that you have not provided in response to the questions above, please provide them here.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Luminant - Luminant Energy	Brenda Hampton	6		Luminant	Brenda Hampton	Luminant - Luminant Energy	6	Texas RE
					Stewart Rake	Luminant Mining Company LLC	7	Texas RE
					Alshare Hughes	Luminant - Luminant Generation Company LLC	5	Texas RE
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
ACES Power Marketing	Brian Van Gheem	6	NA - Not Applicable	ACES Standards Collaborators	Bob Solomon	Hoosier Energy Rural Electric	1	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Cooperative, Inc.		
					Shari Heino	Brazos Electric Power Cooperative, Inc.	1,5	Texas RE
					Ellen Watkins	Sunflower Electric Power Corporation	1	SPP RE
					Mark Ringhausen	Old Dominion Electric Cooperative	3,4	SERC
					Eric Jensen	Arizona Electric Power Cooperative, Inc.	1	WECC
					Ryan Strom	Buckeye Power, Inc.	4	RF
					Susan Sosbe	Wabash Valley Power Association	3	RF
Chris Gowder	Chris Gowder		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utility Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steve Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Mark Brown	City of Winter Park	4	FRCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	9	FRCC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
	Ruida Shu	1,2,3,4,5,6,7,10	NPCC		Paul Malozewski	Hydro One.	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Northeast Power Coordinating Council				RSC no Dominion and OPG	Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Chuck Lawrence	American Transmission Company	1	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Power	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Jeremy Volls	Basin Electric Power Coop	1	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent Independent System Operator	2	MRO
Colorado Springs Utilities	Shannon Fair	6		Colorado Springs Utilities	Kaleb Brimhall	Colorado Springs Utilities	5	WECC
					Charlie Morgan	Colorado Springs Utilities	3	WECC
					Shawna Speer	Colorado Springs Utilities	1	WECC
					Shannon Fair	Colorado Springs Utilities	6	WECC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Megan Wagner	Westar Energy	1,3,5,6	SPP RE

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Robert Gray	Board of Public Utilities (Kansas-BPU)	3	SPP RE
					Steve Keller	Southwest Power Pool Inc.	2	SPP RE
					Tony Eddleman	Nebraska Public Power District	1,3,5	SPP RE
Santee Cooper	Shawn Abrams	1		Santee Cooper	Tom Abrams	Santee Cooper	1	SERC
					Rene' Free	Santee Cooper	1	SERC
					Chris Jimenez	Santee Cooper	1	SERC
					Paul Camilletti	Santee Cooper	5	SERC
					Bob Rhett	Santee Cooper	5	SERC
					Mike Frederick	Santee Cooper	1	SERC
					Troy Lee	Santee Cooper	1	SERC

Summary of Changes
Spelling, formatting, and other errors were corrected.

CIP-003-7(i):
Based on stakeholder comments, the SDT made non-substantive changes to the standard, primarily in the Guidelines and Technical Basis section to provide additional clarity.

Implementation Plan:
No changes made.

Definitions of Transient Cyber Asset and Removable Media:
No changes made.

1. Definition: The SDT revised the definition of Transient Cyber Asset such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Seattle City Light has concerns that the revised definition of Transient Cyber Asset is not consistent with the risk-based approach reflected in the NERC CIP version 5/6 Standards. In particular Seattle finds the revised definition is inconsistent with the language of CIP-002-5.1 R1.3 regarding identification of BES Cyber Systems (and by extension BES Cyber Assets) at Low impact facilities, specifically that: "a discrete list of low impact BES Cyber Systems is not required." Given that the proposed definition defines Transient Cyber Assets in terms of BES Cyber Assets and BES Cyber Systems, Seattle does not understand how the existence of any low impact Transient Cyber Asset can be documented or audited absent a list of such BES Cyber Systems or Assets. Seattle is further concerned that the revised definition could lead to a requirement to produce such lists, which previously has been deemed not consistent with the risk-based approach adopted in CIP version 5/6 (because the development and accurate maintenance of such lists would consume large resources that would provide greater benefits to cyber security if applied elsewhere). At this time Seattle does not have alternative language to suggest to resolve this conundrum, which is inherent to the structure of CIP version 5/6. Perhaps a revision of the definition for Low impact Transient Cyber Asset to reference only a temporary connection "to a BES Cyber System at a low impact facility" might work, but Seattle remains unconvinced that such a definition would prove auditable.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Although the definition of Transient Cyber Asset (TCA) references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required; However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact	

BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Transient Cyber Asset prior to connecting it to a low impact BES Cyber System(s). The security objective of the requirement is to mitigate the risk of introducing malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The requirement lists options but the Responsible Entity has the discretion as to how it satisfies the security objective.	
Julie Hall - Entergy - 6	
Answer	No
Document Name	
Comment	
The proposed definition of Transient Cyber Asset (TCA) implies additional requirements for entities to comply with that is in misalignment with standards that are currently approved and in effect. The purpose of CIP-003-7(i) is to create TCA requirements for Low Impact BES Cyber Systems, yet none of the criteria of item 4 of the definition can be achieved for Lows without imposing additional, and improper, requirements upon the Registered Entities. Item 4 bullets 2 and 3 are omitted because they explicitly require the device or network to be associated with a high or medium impact, leaving just the direct connection to a BES Cyber Asset as the required #4 criteria. However, CIP-002-5.1 R1.3 reads “Identify each asset that contains a low impact BES Cyber System according…if any (a discrete list of low impact BES Cyber Systems is not required).” The requirement explicitly states that a discrete list of BES Cyber Systems is not required. BES Cyber Systems are defined as “One or more BES Cyber Assets logically grouped”, showing that BES Cyber Assets are a sub-componet of a BES Cyber System. CIP-002-5.1 explicitly states that a list of low impact BCS is not required, yet this definition of TCA would require entities to evaluate and inventory, and maintain that inventory, to identify every BES Cyber Asset in order to correctly identify TCA that could be used at a low impact site. Entergy proposes some verbiage to include low impact BCS, while not adding additional inventorying requirements such as “Anticipated for use within a low impact BCS, if any”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Although the definition of Transient Cyber Asset (TCA) references BES Cyber Assets (BCA), a discreet list of BCAs or BES Cyber Systems is not required; However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Transient Cyber	

Asset prior to connecting it to a low impact BES Cyber System(s). The security objective of the requirement is to mitigate the risk of introducing malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The requirement lists options but the Responsible Entity has the discretion as to how it satisfies the security objective. The SDT declines to make the suggested change because it would broaden the scope of the definition and present difficulties in identifying TCAs based on anticipated intent.	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
Since PCA is already defined by NERC, NRG recommends deleting associated with high or medium impact BES Cyber Systems since “associated” could be misunderstood and appears to be redundant. For example, would a VPN connection be considered a TCA? (i.e. connecting at layer 3 or below)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The definitions of PCA and ESP in the published glossary of term does not infer high, medium or low impact categorization. The purpose of the word "associated" with high or medium impact BES Cyber Systems is meant to qualify the impact category of the BES Cyber System and its associated PCA and ESP used in the TCA definition. A VPN connection would not be considered a TCA as it would not be directly connected to a Cyber Asset as item 4 in the definition of TCA specifies.	

Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	

1. We feel the SDT's approach to revise the definition of Transient Cyber Assets (TCA), such that it is relevant to the controls required for high, medium, and low impact BES Cyber Systems, is inconsistent with the directives listed within FERC Order No. 822. These directives focus on the high and medium impact BES Cyber Security requirements. However, the proposed revisions implicitly require low impact entities to have the same level of risk mitigations in places as if they were associated with high and medium impact BES Cyber Systems. We believe the SDT should avoid the inclusion of low impact BES Cyber Systems entirely or provide proof of a risk analysis to substantiate this activity.
2. The SDT's proposed approach will also create difficulty for industry to demonstrate compliance since a BES Cyber System's inventory list is not required for low impact entities. How are auditors able to benchmark a low impact entity's compliance program without a current list?
3. We suggest the SDT consider another method to address the FERC directive that still preserves the low impact requirements and the explicit exclusion from being required to have an inventory list of low impact assets. Such an approach could include TCAs in the technical guidance under Electronic Access Controls.
4. Another possible approach is for low impact entities to have a documented process that applies electronic access controls for TCAs to low impact assets.
    i. Auditors could verify that the entity has developed the documented process, and the entity could demonstrate compliance by providing the document as evidence.
    ii. This approach also preserves the disparate treatment of low and medium impact assets by assigning different requirement levels that commensurate with BES level risks.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. 1. In Order 822 paragraph 32, FERC directs that the CIP standards be modified to "provide mandatory protection for transient devices used at low impact BES Cyber Systems based on the risk posed to Bulk Electric System reliability." The SDT asserts that TCA's connected to low impact BES Cyber Systems must be included to meet the intent of this directive. The SDT asserts that the lower risk of lows was considered and the resulting requirements applied to TCA's that connect to low impact BES Cyber Systems are not as stringent as those for TCA's connected to medium and high impact BES Cyber Systems. 2. In paragraph 36 of Order 822, FERC supports that the controls can "avoid overly burdensome administrative tasks that could be associated with identifying discrete Low Impact BES Cyber Assets" and the standard continues to not require inventories of discrete low impact BES Cyber Assets. The SDT cannot comment on how auditors may approach checking an entity's compliance but in no event is a list of low impact BES Cyber Systems required. 3. Electronic access controls are required to protect external connectivity using routable protocols to the asset; e.g. substation (not connections within the asset or at the individual Cyber Asset level). The SDT disagrees that the electronic access controls section of an entity's plan should mix asset and Cyber Asset level connectivity. 4. The requirement is to have a documented plan as you suggest, but the plan would not address electronic access controls for TCAs. The relevant section of the plan for TCAs should address mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media.

Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	
Comment	
Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Transient Cyber Asset definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.	

The definition does not spell out what defines a TCA in a low impact environment. Should the definition include additional instruction related to item 4 such as “connected to a cyber asset located in an asset contiaing low impact BES Cyber Systems”?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. 1. In Order 822 paragraph 32, FERC directs that the CIP standards be modified to "provide mandatory protection for transient devices used at low impact BES Cyber Systems based on the risk posed to Bulk Electric System reliability." The SDT asserts that TCA's connected to low impact BES Cyber Systems must be included to meet the intent of this directive. The SDT asserts that the lower risk of lows was considered and the resulting requirements applied to TCA's that connect to low impact BES Cyber Systems are not as stringent as those for TCA's connected to medium and high impact BES Cyber Systems. 2. In paragraph 36 of Order 822, FERC supports that the controls can "avoid overly burdensome administrative tasks that could be associated with identifying discrete Low Impact BES Cyber Assets" and the standard continues to not require inventories of discrete low impact BES Cyber Assets. The SDT cannot comment on how auditors may approach checking an entity's compliance but in no event is a list of low impact BES Cyber Systems required. 3. Electronic access controls are required to protect external connectivity using routable protocols to the asset; e.g. substation (not connections within the asset or at the individual Cyber Asset level). The SDT disagrees that the electronic access controls section of an entity's plan should mix asset and Cyber Asset level connectivity. 4. The requirement is to have a documented plan as you suggest, but the plan would not address electronic access controls for TCAs. The relevant section of the plan for TCAs should address mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media.	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	No
Document Name	

Comment	
In the current TCA definition, section 4, first bullet: If the intent of the definition for "BES Cyber Asset" to be applicable for all three impact classifications (High, Medium, and Low), then SDG&E recommends adding this clarification.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT contends the definition needs to describe what a TCA is regardless of its impact rating. Impact ratings are taken into account within respective requirements for highs, mediums, and lows.	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Transient Cyber Asset definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT included the referenced language in the definitions to specifically address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems. No additional guidance is required.	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy would like to point out a possible typo on page 3 of the Proposed Definitions of: Transient Cyber Asset"(TCA) and "Removable Media" document. The title of the section on page 3 reads "Currently Approved Definition of Transient Cyber Asset (TCS)". The definition below is actually the definition of Removable Media. The title appears to be incorrect. We recommend the drafting team change the title to read: *"Currently Approved Definition of Removable Media".*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT made the modification.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes 0	
Dislikes 0	

Response	
Please see the SDT's responses to comments submitted by APPA.	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT’s responses to comments submitted by APPA.	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Add a « Low impact BES » item in the TCA definition. This will exempt the inventory requirement for low to demonstrate compliance for the TCA. The proposed definition of a Transient Cyber Asset (TCA) is: *A Cyber Asset that is:* *1. capable of transmitting or transferring executable code,* *2. not included in a BES Cyber System,* *3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and*	

4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: *BES Cyber Asset,* *Add "Low impact BES Cyber System",* *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or* *PCA associated with high or medium impact BES Cyber Systems.*

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The definition of Transient Cyber Asset (TCA) references BES Cyber Assets (BCAs) regardless of impact level. A BES Cyber System is defined as "One or more BES Cyber Assets…" therefore, the SDT disagrees with adding the proposed text.

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment
It would be helpful if the revised definitions could be reorganized to provide the inclusions first and the exclusions second to make them easier to read and implement. For example, the TCA definition could be changed to: "A Cyber Asset that is: 1) capable of transmitting or transferring executable code; 2) directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: BES Cyber Asset, network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or PCA associated with high or medium impact BES Cyber Systems; 3) not included in a BES Cyber System; and 4) not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems. Examples..."

Also, the applicability of the definitions to LIBCS is not clear, we recommend changing “BES Cyber Asset” in bullet 4 for each definition to “BES Cyber System” or alternatively “low, medium, or high impact BES Cyber System.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The revisions to the definitions were only to clarify applicability to low impact. The structure is consistent with the currently approved definition. The definition of Transient Cyber Asset (TCA) references BES Cyber Assets (BCAs) regardless of impact level. A BES Cyber System is defined as "One or more BES Cyber Assets…” therefore, the SDT disagrees that adding the proposed text or rearranging the order of the definition would improve clarity.	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 – NPCC	
Answer	Yes
Document Name	
Comment	
Suggest to add a « Low impact BES » item in the TCA definition. This will exempt the inventory requirement for low to demonstrate compliance for the TCA. The proposed definition of a Transient Cyber Asset (TCA) is: *A Cyber Asset that is:* *1. capable of transmitting or transferring executable code,* *2. not included in a BES Cyber System,* *3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and*	

4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • *BES Cyber Asset,* • *Add "Low impact BES Cyber System",* • *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or* • *PCA associated with high or medium impact BES Cyber Systems.*

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The definition of Transient Cyber Asset (TCA) references BES Cyber Assets (BCAs) regardless of impact level. A BES Cyber System is defined as "One or more BES Cyber Assets…" therefore, the SDT disagrees with adding the proposed text.

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	

Comment
Santee Cooper agrees with APPA's comment/concern.

Likes 0	
Dislikes 0	

Response
Please see the SDT's responses to comments submitted by APPA.

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Transient Cyber Asset definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT included the referenced language in the definitions to specifically address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems. No additional guidance is required.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Bobby Olsen - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike Anctil - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	

2. Definition: The SDT revised the definition of Removable Media such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	No
Document Name	
Comment	
In the proposed Removable Media definition, section 4, first bullet: If the intent of the definition for "BES Cyber Asset" to be applicable for all three impact classifications (High, Medium, and Low), then SDG&E recommends adding this clarification.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT contends the definition needs to describe what Removable Media is regardless of its impact rating. Impact ratings are taken into account within respective requirements for highs, mediums, and lows.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	
Comment	
Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Removable Media definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified. The definition does not spell out what defines RM in a low impact environment. Should the definition include additional instruction related to item 4 such as "connected to a cyber asset located in an asset contiaing low impact BES Cyber Systems"?	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT included the referenced language in the definitions to specifically address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems. No additional guidance is required.	
Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	

1. Similar to TCAs, we suggest the SDT revise its approach and remove low impact BES Cyber Security requirements from the definition of Removable Media (RM). We feel its relevance on controls required for high, medium, and low impact BES Cyber Systems is not the best way to address the directives listed in FERC Order No. 822. The proposed revisions implicitly require low impact entities to have the same level of risk mitigiations in places as if they were associated with high and medium impact BES Cyber Systems. We believe the SDT should avoid the inclusion of low impact BES Cyber Systems entirely or provide proof of a risk analysis to substatntiate this activity.
2. We suggest the SDT consider another method to address the FERC directive that still preserves the low impact requirements and the explicit exclusion from being required to have an inventory list of low impact assets. Such an approach could include Removable Media in the technical guidance under Electronic Access Controls that are currently approved.
3. One possible approach is for low impact entities to have a documented process that applies electronic access controls for Removable Media to low impact assets.
    i. Auditors could verify that the entity has developed the documented process, and the entity could demonstrate compliance by providing the document as evidence.
    ii. This approach also preserves the disparate treatment of low and medium impact assets by assigning different requirement levels that commensurate with BES level risks

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. 1. In Order 822 paragraph 32, FERC directs that the CIP standards be modified to ""provide mandatory protection for transient devices used at low impact BES Cyber Systems based on the risk posed to Bulk Electric System reliability."" The SDT asserts that Removable Media connected to low impact BES Cyber Systems must be included as a transient device to meet the intent of this directive. 2. In paragraph 36 of Order 822, FERC supports that the controls can "avoid overly burdensome administrative tasks that could be associated with identifying discrete Low Impact BES Cyber Assets" and the standard continues to not require inventories of discrete low impact BES Cyber Assets. The SDT cannot comment on how auditors may approach checking an entity's compliance, but a list of low impact BES Cyber Systems is not required. 3. The requirement is to have a documented plan as you suggest, but the plan would not address electronic access controls for Removable Media. The relevant section of the plan for Removable Media should address mitigating the risk of the introduction of malicious code into low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media.	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
Since PCA is already defined by NERC, NRG recommends deleting associated with high or medium impact BES Cyber Systems since “associated” could be misunderstood and appears to be redundant.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

The definitions of PCA and ESP in the published glossary of term does not infer high, medium or low impact categorization. The purpose of the word "associated" with high or medium impact BES Cyber Systems is meant to qualify the impact category of the BES Cyber System and its associated PCA and ESP used in the Removable Media definition. The SDT included the referenced language specifically to address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems.	
Julie Hall - Entergy - 6	
Answer	No
Document Name	
Comment	
The proposed definition of Removable Media (RM) implies additional requirements for entities to comply with that is in misalignment with standards that are currently approved and in effect. The purpose of CIP-003-7(i) is to create RM requirements for Low Impact BES Cyber Systems, yet none of the criteria of item 4 of the definition can be achieved for Lows without imposing additional, and improper, requirements upon the Registered Entities. Item 4 bullets 2 and 3 are omitted because they explicitly require the device or network to be associated with a high or medium impact, leaving just the direct connection to a BES Cyber Asset as the required #4 criteria. However, CIP-002-5.1 R1.3 reads “Identify each asset that contains a low impact BES Cyber System according…if any (a discrete list of low impact BES Cyber Systems is not required).” The requirement explicitly states that a discrete list of BES Cyber Systems is not required. BES Cyber Systems are defined as “One or more BES Cyber Assets logically grouped”, showing that BES Cyber Assets are a sub-componet of a BES Cyber System. CIP-002-5.1 explicitly states that a list of low impact BCS is not required, yet this definition of TCA would require entities to evaluate and inventory, and maintain that inventory, to identify every BES Cyber Asset in order to correctly identify RM that could be used at a low impact site. Entergy proposes some verbiage to include low impact BCS, while not adding additional inventorying requirements such as “Anticipated for use within a low impact BCS, if any”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Although the definition of Removable Media references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required; However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Removable Media prior	

to connecting it to a low impact BES Cyber System(s). The security objective of the requirement is to mitigate the risk of introducing malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The requirement lists options but the Responsible Entity has the discretion as to how it satisfies the security objective. The SDT declines to make the suggested change because it would broaden the scope of the definition and present difficulties in identifying Removable Media based on anticipated intent.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
As is the case for the revised Transiet Cyber Asset definition, Seattle City Light has concerns that the revised definition of Removable Media is not consistent with the risk-based approach reflected in the NERC CIP version 5/6 Standards. In particular Seattle finds the revised definition is inconsistent with the language of CIP-002-5.1 R1.3 regarding identification of BES Cyber Systems (and by extension BES Cyber Assets) at Low impact facilities, specifically that: “a discrete list of low impact BES Cyber Systems is not required.” Given that the proposed definition defines Removable Media in terms of BES Cyber Assets and BES Cyber Systems, Seattle does not understand how the existence of any low impact Removable Media can be documented or audited absent a list of such BES Cyber Systems or Assets. Seattle is further concerned that the revised definition could lead to a requirement to produce such lists, which previously has been deemed not consistent with the risk-based approach adopted in CIP version 5/6 (because the development and accurate maintenance of such lists would consume large resources that would provide greater benefits to cyber security if applied elsewhere). At this time Seattle does not have alternative language to suggest to resolve this conundrum, which is inherent to the structure of CIP version 5/6. Perhaps a revision of the definition for Low impact Removable Media to reference only a temporary connection “to a BES Cyber System at a low impact facility” might work, but Seattle remains unconvinced that such a definition would prove auditable.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Although the definition of Removable Media references BES Cyber Assets (BCA), a discreet list of BCAs or BES Cyber Systems is not required; However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES	

Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Removable Media prior to connecting it to a low impact BES Cyber System(s). The security objective of the requirement is to mitigate the risk of introducing malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The requirement lists options but the Responsible Entity has the discretion as to how it satisfies the security objective.	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Removable Media definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT included the referenced language in the definitions to specifically address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems. No additional guidance is required.	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	

Comment	
Santee Cooper agrees with APPA's comment/concern.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by APPA.	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	

Suggest to dd a « Low impact BES » item in the TCA definition. This will exempt the inventory requirement for low to demonstrate compliance for the TCA.

The proposed definition of Removable Media is:

Storage media that:

1. *are not Cyber Assets,*
2. *are capable of transferring executable code,*
3. *can be used to store, copy, move, or access data, and*
4. *are directly connected for 30 consecutive calendar days or less to a:*
    - *BES Cyber Asset,*
    - *Low impact BES Cyber System,*
    - *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*

o *Protected Cyber Asset associated with high or medium impact BES Cyber Systems.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The definition of Removable Media references BES Cyber Assets (BCAs) regardless of impact level. A BES Cyber System is defined as "One or more BES Cyber Assets…" therefore, the SDT disagrees with adding the proposed text.	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Add a « Low impact BES » item in the TCA definition. This will exempt the inventory requirement for low to demonstrate compliance for the TCA. The proposed definition of Removable Media is: *Storage media that:* 5. *are not Cyber Assets,* 6. *are capable of transferring executable code,* 7. can *be used to store, copy, move, or access data, and* 8. are directly *connected for 30 consecutive calendar days or less to a:* *BES Cyber Asset,* *Low impact BES Cyber System,*	

network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or *Protected Cyber Asset associated with high or medium impact BES Cyber Systems.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The definition of Removable Media references BES Cyber Assets (BCAs) regardless of impact level. A BES Cyber System is defined as "One or more BES Cyber Assets…" therefore, the SDT disagrees with adding the proposed text.	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by APPA.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes 0	

Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by APPA.	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Removable Media definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT included the referenced language specifically to address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems.	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	

Comment	
The term “transferring code” is misleading because the device itself (for example, storage media) cannot transfer code without assistance from the host computer.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. As stated in the definition, the Removable Media is capable of transferring executable code regardless of whether the host computer assists or not; consequently, no changes to the definition are necessary.	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Anctil - Los Angeles Department of Water and Power - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobby Olsen - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment	
Texas RE noticed the TCA definition includes examples of what directly connected means, "*directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a*". There are no examples for "directly connected" listed in the Removable Media definition. Texas RE recommends that the SDT provide examples to provide clarity to the industry. There are instances when removable media may be physically directly connected but not active until mounted.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT contends that examples of "directly connected" are not necessary for Removable Media. The entity should scan all Removable Media prior to connecting to the BCA whether the Removable Media is mounted or not.	

3. Requirement R2: The SDT revised CIP-003-7(i), Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to mitigate the risk of propagation of malware from transient devices. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

The NSRF clearly understands that all entities regardless of size can be the door way for malicious code to entire into the BES systems. This includes small entities with one Low Impact BES Cyber Systems only (read low risk) (maybe a generator, one Transmission sub station, or control system). With this is mind, the NSRF has the following concerns that the SDT should clarify for all entities with Low Impact BES Cyber Systems.

The NSRF has concerns with Attachment 1, part 5.2 for entities that have Low Impact BES Cyber Systems, only. The actionable items in 5.2 is for us the entity to "Review" items that the "other party" needs to do to do prior to connecting to our Low Impact BES Cyber System. Please clariy what "review" means? What is acceptable within our review process? Attachment 2 states examples of electronic mail, policies, contracts, etc. Do we just review that the "other party" states that they will accomplish the attributes of 5.2 and have that stated within a contract, e-mail, STOW, etc. and we are compliant? This will play a role with proprietary software when a vendor will not provide associated evidence.

This clarity will reduce the compliance risks for the small entity and will assure that entities meet the attributes of 5.2, thus maintaining a secure BPS.

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

• Antivirus software, including manual or managed updates of signatures or patterns;

• Application whitelisting; or

• Other method(s) to mitigate the introduction of malicious code. Please clarify how the SDT wishes to use the semicolon within the first bullet of 5.1? Does this mean “and” or “or” as in the second bullet? We have the same question for all semicolons in 5.2 as well. The NSRF believes by adding a simple “or” after each semicolon, we will clearly know what the intent of the bulleted items are.	
Likes 1	Georgia Transmission Corporation, 1, Snodgrass Jason
Dislikes 0	
Response	
Thank you for your comments. Specific approaches on how to perform the review could be submitted as Implementation Guidance in accordance with NERC Compliance Guidance Policy. According to the background sections of the CIP standards, the use of the semicolon and the "or" is consistent with the usage in all standards. A bulleted list means an "or" and a numbered list means "and."	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
The language is open ended and fails to provide discrete direction to entities on how to implement a plan. This will lead to subjective enforcement, with the possibility for significant discrepancies and differences between regions.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT notes that the requirement allows entities the flexibility to develop and implement the plan(s) appropriate for the entity's environment.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Seattle City Light agrees with the revisions so far as they go, but finds that they do not address the question of what would be acceptable evidence of the existence of any Low impact Transient Cyber Asset (based on the proposed definition) in the absence of an explicit list of Low impact BES Cyber Systems and Assets at a facility. As discussed in the definition comment above, Seattle does not have a solution to the problem, which is inherent to the structure of CIP verion 5/6.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to your Question 1 comment.	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
This is a low impact requirement rather than a high or medium impact requirement. While risks of malicious code are definitely present, the reduced risk level would make this entire requirement more effective by requiring the entity document and implement a security program with appropriate controls that prevent introduction of malicious code. Examples of appropriate controls are: application	

whitelisting, antivirus, use of bootable CDs without known malware, contracts with vendors, etc. Note that use of third party TCA is expected to be much more frequent on low impact BCS and highly presecriptive requirements are less effective. Should the above approach not be acceptable, requirement 5.3.1 and 5.3.2 should be consolidated into a single statement. A requirement to scan prior to connecting and then separately document and mitigate is redundant. The Removable media simply needs to be clean prior to connecting to a Transient Cyber Asset. Seminole suggests making that the requirement. For example, the language could be modified to state: For Removable Media, document and implement methods that prevent the introduction of malicious code on BES Cyber Assets when connecting Removable Media. In cases of detected malicious code that cannot be removed, the entity shall document how the identified malware is mitigated.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT notes that the requirement allows entities to implement a security program as suggested by your comment and includes the flexibility to develop a single plan for implementing Attachment 1, Sections 5.3.1 and 5.3.2.	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	No
Document Name	
Comment	
ITC Holdings agrees with the comment submitted by NSRF – see below: The NSRF clearly understands that all entities regardless of size can be the door way for malicious code to entire into the BES systems. This includes small entities with one Low Impact BES Cyber Systems only (read low risk) (maybe a generator, one Transmission sub station, or control system). With this is mind, the NSRF has the following concerns that the SDT should clarify for all entities with Low	

Impact BES Cyber Systems. The NSRF has concerns with Attachment 1, part 5.2 for entities that have Low Impact BES Cyber Systems, only. The actionable items in 5.2 is for us the entity to “Review” items that the “other party” needs to do to do prior to connecting to our Low Impact BES Cyber System. Please clariy what “review” means? What is acceptable within our review process? Attachment 2 states examples of electronic mail, policies, contracts, etc. Do we just review that the “other party” states that they will accomplish the attributes of 5.2 and have that stated within a contract, e-mail, STOW, etc. and we are compliant? This will play a role with proprietary software when a vendor will not provide associated evidence. This clarity will reduce the compliance risks (burden) for the small entity and will assure that entities meet the attributes of 5.2. 5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability): • Antivirus software, including manual or managed updates of signatures or patterns; • Application whitelisting; or • Other method(s) to mitigate the introduction of malicious code. Please clarify how the SDT wishes to use the semicolon within the first bullet of 5.1? Does this mean “and” or “or” as in the second bullet? We have the same question for all semicolons in 5.2 as well. The NSRF believes by adding a simple “or” after each semicolon, we will clearly know what the intent of the bulleted items are.	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. Specific approaches on how to perform the review could be submitted as Implementation Guidance in accordance with NERC Compliance Guidance Policy. According to the background sections of the CIP standards, the use of the semicolon and the "or" is consistent with the usage in all standards. A bulleted list means an "or" and a numbered list means "and."
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment
MMWEC supports the comments submitted by Georgia Transmission Corp. regarding streamling Section 5 by moving the bullets to GTB and keeping the security objective in the Attachment.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The use of the bulleted list is consistent with other currently approved standards. The SDT's intention in using the bulleted list is to provide options to satisfy the parent statement, and the SDT purposely included the ability for the Responsible Entity to use other protection methods, rather than those listed, that more adequately fit the entity's environment.
Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators

Answer	No
Document Name	

Comment

1. We have concerns with part 5.2 of Attachment 1 for applicable entities that only have Low Impact BES Cyber Systems. Many of these entities provide a small risk to the BES since they only have one low impact BES Cyber Systems (e.g. a generator, one Transmission substation, or a single control system). Will Regional Entities conduct the same audit for small entities as they would for large multi-regional corporate companies? What is the impact when a vendor does not comply with the request listed in part 5.2?
2. We also question the need for additional explicit requirements to validate vendor security and patch management plans as part of a low impact entity's cyber security policies. We believe these requirements are already incorporated in an entity's Electronic Access Controls Policy. These additional requirements are a burden to existing low impact entities that may only have one or two TCA-applicable or RM-applicable BES cyber assets. We recommend removing these requirements for low Impact entities until after the effective date for NERC Reliability Standard CIP-007-3 (i.e. September 1, 2018).
3. The inclusion of TCA and RM with the final definition of LERC is unnecessary. We don't agree with the SDT's approach of posting two options, and then recommend the all-inclusive option over the other. The SDT should wait for industry to provide feedback on both options or post only one path forward and determine if industry supports it. The one option adds additional risk for ballot approval.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

The SDT cannot comment on the manner in which audits will be conducted by the Regional Entities. Compliance with the requirements is the responsibility of the entity being audited. In Attachment 1, Section 5, Part 5.2, the intention of the SDT is to provide options that a Responsible Entity can employ to ensure TCAs managed by third parties do not present additional risk to the BES. Please refer to example evidence in Attachment 2 for possible options.

If a Responsible Entity's Electronic Access Control Policy is able to mitigate the risk of the introduction of malware via TCAs, the Responsible Entity can utilize this as such and present that to auditors. The SDT intentionally ensured this requirement was not prescriptive to allow an entity to provide appropriate protections per their environment.

The SDT's objective is to minimize the number of revisions.	
Mike Anctil - Los Angeles Department of Water and Power - 3	
Answer	No
Document Name	
Comment	
This NERC project is adding a new Section 5 bringing into scope Transient Cyber Assets and Removable Media for Low Impact Facilities which is a much larger scope than our High and Medium Impact Program without any extension of time for compliance indicated for implementation. This will be impactful to the Power System.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The intention of the SDT is to give Responsible Entities more flexibility at Lows than is currently allowed at Highs or Mediums while satisfying the FERC 822 directive. An entity can choose to utilize the same programs currently implemented for Highs and Mediums to meet the security objective for Lows. The implementation period for CIP-003-7(i) is 18 months.	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation appreciates the Standards Drafting Team's consideration of prior recommendations. Reclamation agrees with the changes and has the following question: In this version of CIP-003-7(i), did the SDT intend to add guidance regarding the new section on page 9 under Requirement 1 "1.2.6 Declaring and responding to CIP Exceptional Circumstances" in Attachment 1 and/or Attachment 2?	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT added G&TB language for Requirement R1, Part 1.2.6.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE's appreciates the SDT's efforts to implement the FERC directive in Order No. 822 to "develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to the bulk electric system reliability." In implementing this directive, Texas RE notes that the SDT appears to have used the existing Transient Cyber Asset (TCA) and Removable Media requirements for medium and high impact BES Cyber Systems and associated Protected Cyber Assets set forth in CIP-10-2, Attachment 1, Sections 1 through 3 as the basis for developing the new TCA and removable media requirements for low impact BES Cyber Systems. While Texas RE agrees with this general approach, Texas RE notes that the SDT elected to not include all applicable requirements. For instance, the current draft of CIP-003, Attachment 1, Section 5 omits any requirements to mitigate software vulnerabilities (CIP-10-2, Attachment 1, Section 1.3 for TCAs managed by the Responsible Entity; CIP-10-2, Attachment 1, Section 2.1 for TCAs managed by a party other than the Responsible Entity). Texas RE requests that the SDT provide its risk-based justification for why those aspects of the CIP-010-2, Attachment 1 requirements for medium and high impact TCAs and removable media are not correspondingly extended to similar low impact devices. Among other things, this will assist Texas RE in its efforts to understand, evaluate, and ensure compliance with the new low impact requirements. In addition, Texas RE noticed the following: • There is no distinction provided for Removable Media used by different parties. Was that the intent of the SDT? As written it appears to be for any Removable Media used by any party (e.g., vendor, or third party technician/personnel).	

• Texas RE recommends that the SDT specifically address the impact of backup tapes, libraries, and drives. More specifically Texas RE recommends addressing magnetic tapes, in regard to section 5.3.2. How would an entity mitigate the threat of detected malicious code on magnetic tapes prior to connecting it to a high, medium, or low impact BES Cyber System? • On Page 29, Section 5 - Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation; there is an extra "_" that is not needed after the colon symbol.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In the assessment of risk, one factor is the impact or consequence of the realization of the risk. The SDT notes that the risk related to the introduction of malicious code is less for low impact BES Cyber Systems than medium or high impact BES Cyber Systems. This is because, by definition, the impact is less. As such, the SDT selected a reduced set of controls for low impact that directly address the concern that transient devices are potentially more susceptible to malicious code due to connections to different systems and networks. FERC Order 822 directed that the requirements be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards. Yes, the intent of the SDT was not to create a distinction for third-party Removable Media. However, there is no language in Attachment 1 that would prevent an entity from making such a distinction in its own plan so long as the methods chosen meet the security objective identified in Section 5 of Attachment 1.	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	

Comment
1) The bulleted list creates requirements that are too prescriptive. Use alternative language for Section 5.1 and 5.2 to remove the bullet points (because they may be used against you in some fashion in the future), and re-write the requirements. The bullet points should go into the GTB section so that there is less chance for a misinterpretation of reinterpretation that would require the implementation of more than one of the bulleted point in order to meet compliance. 2) As written, the requirements listed for TCAs in CIP-003-7(i) for Low Impact assets is a subset of the requirements for high and medium impact included in CIP-010-2 R4. As is or if changed the GTB section should include a statement the low impact requirements are a subset of those for High and Medium.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The use of the bulleted list is consistent with other currently approved standards. The SDT's intention in using the bulleted list is to provide options to satisfy the parent statement, and the SDT purposely included the ability for the Responsible Entity to use other protection methods, rather than those listed, that more adequately fit the entity's environment. The relationship between highs, mediums, and lows is addressed in Attachment 1 to allow entities to utilize a single program for all impact levels.

Julie Hall - Entergy - 6	
Answer	Yes
Document Name	

Comment
Agree with CIP-003-7(i), Attachment 1, Section 5 as written in this draft. As written, this verbiage implies entities has latitude to implement a strategy based on a risk to achieve the goal of the standard. See response to question 4 below for concerns regarding actual implementation of plans.

Likes 1	Georgia Transmission Corporation, 1, Snodgrass Jason
Dislikes 0	
Response	
Thank you for your comment.	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	

Exelon supports the changes made to CIP-003-7(i), R2, Attachment 1, adding Section 5; however, we request the SDT consider the following adjustments:

1. The language in Attachment 1, Section 5, regarding "achieve the objective of mitigating the risk of the introduction of malicious code," differs from the language in CIP-010-2, R4, Attachment 1, Section 1.3, which states "…achieves the objective of mitigating the introduction of…" Exelon requests the SDT consider aligning the two obligations to the language found in CIP-010-2, R4 or add clarification to the Guidelines and Technical Basis that provides clarity regarding the addition of "...the risk of…" and whether there are any additional or different expectations for Responsible Entities related to CIP-003-7(i), R2. Exelon is concerned that the addition of "risk" could be interpreted to require performing and documenting a risk assessment of all of the risks posed by the introduction of malicious code.

The following sentence (or something comparative) could be added to the Guidelines and Technical Basis as the last sentence in the first paragraph related to Section 5.1 if the SDT determines the requirement language does not require alignment: "When determining the method(s) to mitigate the introduction of malicious code, it is not intended Responsible Entities have to perform and document a risk assessment to determine all of the risks associated with the introduction of malicious code."

1. Attachment 1, Section 5.3.2 states, "Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System." Exelon proposes a one-word change to replace the "…threat of…" to "…threat from…" This minor wording change helps to clarify the meaning of the obligation. Using the word "from" makes it clear that the mitigation of the threat is associated with already detected malicious code, as opposed to mitigation of a general threat of malicious code that may occur in the future.

Likes 0	
Dislikes 1	Georgia Transmission Corporation, 1, Snodgrass Jason

Response

Thank you for your comments.

The SDT does not intend for entities to perform a risk assessment and added the recommended language to the G&TB.

The SDT asserts that the use of the word "and" at the end of Attachment 1, Section 5, Part 5.3.1 clarifies what is to be mitigated in Attachment 1, Section 5, Part 5.3.2.

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities

Answer	Yes
Document Name	

Comment

1) The bulleted list creates requirements that are too prescriptive. Use alternative language for Section 5.1 and 5.2 to remove the bullet points (because they may be used against you in some fashion in the future), and re-write the requirements. The bullet points should go into the GTB section so that there is less chance for a misinterpretation of reinterpretation that would require the implementation of more than one of the bulleted point inorder to meet compliance.

2) As written, the requirements listed for TCAs in CIP-003-7(i) for Low Impact assets is a subset of the requirements for high and medium impact included in CIP-010-2 R4. As is or if changed the GTB section should include a statement the low impact requirements are a subset of those for High and Medium.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

1. The use of the bulleted list is consistent with other currently approved standards. The SDT's intention in using the bulleted list is to provide options to satisfy the parent statement, and the SDT purposely included the ability for the Responsible Entity to use other protection methods, rather than those listed, that more adequately fit the entity's environment. 2. The SDT notes that the requirement allows entities to implement a security program as suggested by your comment and includes the flexibility to develop a single plan for implementing Attachment 1, Section 5, Parts 5.3.1 and 5.3.2.	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Comments: Both sections 5.1 and 5.2 contain an option of “Other method(s) to mitigate the introduction of malicious code” which grants responsible entities flexibility in choosing alternative methods not included in the list of bulleted items as long as the methods achieve the core security objective outlined in section 5. Therefore, it seems that emphasis is placed on achieving the security objective established by the core of section 5 and the distinction between 5.1 and 5.2 is for the plan to include and cover whom is managing TCAs and not specificly to capture the various options bulleted within the required plan. As such, GTC believes the bullet point “options” introduces unneccesary prescriptive language and can be removed from the requirements without changing the intent of the requirement whatsoever and the drafting team could simplify with and affirmative ballot. GTC recognizes these options provide contextual ideas of how one could go about achieving the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems and further recommends that they be relocated into the guidelines and technical basis of the standard. This streamlined revision to section 5 could be simplified for clarity of implementation on the front end and clarity of compliance testing on the audit end as follows: Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include: 5.1 Method(s) to mitigate the introduction of malicious code for Transient Cyber Asset(s) managed by the Responsible Entity, if any.	

5.2 Method(s) to mitigate the introduction of malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any. 5.3 For Removable Media, the use of each of the following: 5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and 5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The use of the bulleted list is consistent with other currently approved standards. The SDT's intention in using the bulleted list is to provide options to satisfy the parent statement, and the SDT purposely included the ability for the Responsible Entity to use other protection methods, rather than those listed, that more adequately fit the entity's environment.	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy would like to see added clarification within the Guidelines and Technical Basis around the concept of an acceptable review of a 3rd party vendors malware mitigation mechanisms. Currently, in Section 5.2 of Attachment 1, a Responsible Entity is required to "Review" one or a combination of the malware mitigation mechanisms of a 3rd party vendor. Our concern is that it is unclear what constitutes an acceptable "review" of these mechanisms. It is possible that what is considered an acceptable review by one entity, may not be considered acceptable by another. We suggest the drafting team consider adding language to the Guidelines and Technical Basis further describing what constitutes an acceptable review.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Specific approaches on how to perform the review could be submitted as Implementation Guidance in accordance with NERC Compliance Guidance Policy.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT’s responses to comments submitted by APPA.	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	Yes
Document Name	
Comment	
We like to see examples how to have the ability to restrict malware to the TCA's. Also like to see some examples around technical guidance and mitigation plans. Possibly adding administrative control methods in the technical basis sections for transient devices. Add language in the technical basis restricting movement of TCA's.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The "other" category is intended to allow for future technology or accommodate approaches not considered during the development of the standard. Specific approaches could be submitted as implementation guidance at any point in the future.	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA. In Attachment 1, Section 5, 5.2, what frequency is intended by the words "prior to"? Is this intended to be once upon execution of a vendor/contractor support contract, or is it intended to be at some other interval/frequency?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Per the G&TB for Attachment 1, Section 5, Part 5.2; there is no specific frequency of performance, and the G&TB states "The use of “prior to connecting the Transient Cyber Assets” is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code...the SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective."	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	

Comment	
Summary of changes in page 44 of the guidelines CIP010 mentioned : “All requirements related to TCA and RM are included within a single standard, CIP010. But requirements exist also in CIP-003-07 R2 . HQP suggest to modify the summary of changes. The word “Managed” should be in lower case for paragraph in the page 56 of 62 “**Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity”**. It could be usefull to introduce base of risk in the case of a TCA connected to LOW impact BES systems without external connectivity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT includes requirements for TCAs and RM for Lows in CIP-003 to remain consistent with Attachment 1 of CIP-003, which is devoted to protections around Low Impact Assets. The term "Managed" is capitalized here because the term is part of the title of the section. Although not required, the proposed requirements allow an entity to assess risk based on external connectivity. Regardless of external connectivity, the SDT asserts that per FERC Order 822, a Responsible Entity must develop a plan around mitigating the risk of introducing malicious code to low impact BES Cyber Systems.	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Summary of changes in page 44 of the guidelines CIP010 mentioned :	

"All requirements related to TCA and RM are included within a single standard, CIP010. But requirements exist also in CIP-003-07 R2 . HQP suggest to modify the summary of changes. The word "Managed" should be in lower case for paragraph in the page 56 of 62 "**Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity"**. It could be usefull to introduce base of risk in the case of a TCA connected to LOW impact BES systems without external connectivity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT includes requirements for TCAs and RM for Lows in CIP-003 to remain consistent with Attachment 1 of CIP-003, which is devoted to protections around Low Impact Assets. The term "Managed" is capitalized here because the term is part of the title of the section. Although not required, the proposed requirements allow an entity to assess risk based on external connectivity. Regardless of external connectivity, the SDT asserts that per FERC Order 822, a Responsible Entity must develop a plan around mitigating the risk of introducing malicious code to low impact BES Cyber Systems.	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Santee Cooper agrees with APPA's comments.	
Likes 0	
Dislikes 0	

Response	
Please see the SDT’s responses to comments submitted by APPA.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Recommend revisions to remove the bulleted list and re-write the requirements. The bullet points should go into the GTB section so that there is less chance for a misinterpretation that would require the implementation of more than one of the bulleted point in order to meet compliance.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The use of the bulleted list is consistent with other currently approved standards. The SDT's intention in using the bulleted list is to provide options to satisfy the parent statement, and the SDT purposely included the ability for the Responsible Entity to use other protection methods, rather than those listed, that more adequately fit the entity's environment.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobby Olsen - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
We continue to have concerns about how the GTB are factored into Compliance and Enforcement. In some cases it appears that they create “requirements” that must be incorporated into your program; this is inconsistent with prior FERC precedent. On the other hand, it is not clear whether or not you can rely on the GTB in developing your program and ensuring compliance. This concern continues to fail to be addressed by the SDT. With respect to Attachment 1 Section 3, and Attachment 2, Section 3.1, it doesn't make sense to keep referring to physical location when it comes to electronic controls (as previously noted).	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. The G&TB provides SDTs a mechanism to: (i) explain the technical basis for the associated Reliability Standard (and Requirements therein); and (ii) provide technical guidance to help support effective application of the associated Reliability Standard. As provided in the response to draft 2 of CIP-003-7, the requirement language does not prescribe a physical versus logical approach to the implementation. The use of the term "asset" refers to assets identified as containing low impact BES Cyber System(s) pursuant to CIP-002. As described in the G&TB, the Responsible Entity has the flexibility to identify the electronic boundary surrounding the low impact BES Cyber System rather than using a physical boundary.

4. Attachment 2: The SDT revised the evidential language of CIP-003-7(i), Attachment 2, Section 5 to make the Measures consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	
Comment	
The complexity of the sentences are difficult to read and understand. Suggest revising to bulleted lists. The evidence requirements seem to require an inventory of TCA's and RM. This could be an issue in the same way that a list of BES Cyber Systems has been determined to be an issue.	
Likes 0	
Dislikes 0	
Response	
While the SDT thanks you for the comment, we decline to make the suggested modification to the format. Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required. However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Removable Media prior to connecting it to a low impact BES Cyber System(s).	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	

Comment	
Reclamation appreciates the Standards Drafting Team's consideration of prior recommendations. Reclamation agrees with the changes and has the following question: In this version of CIP-003-7(i), did the SDT intend to add guidance regarding the new section on page 9 under Requirement 1 "1.2.6 Declaring and responding to CIP Exceptional Circumstances" in Attachment 1 and/or Attachment 2?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT added G&TB language for Requirement R1, Part 1.2.6.	
Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
We disagree with the proposed language, as the SDT has only restated the content of the requirement language. There is no process or guidance for an entity to follow when a vendor fails to comply with required request. Is a vendor's attestation sufficent proof for an entity to demonstrate reasonable assurance for compliance? If so, an attestation should be included in the list of acceptable evidence for this requirement, and reflected in Attachment 2 to ensure consistent regional application.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

The SDT notes that the requirement allows entities the flexibility to develop and implement the plan(s) appropriate for the entity's environment. The evidence that an entity will need to utilize will be dependent on the plan that is in place to mitigate the threat of introduction of malicious code at Lows.	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
This change creates additional requirements for Low Impact BCS relating to change control (additional cost implications from an administrative standpoint with limited reliability benefit) (i.e. capture every time a TCA is connected to a system and this infers that an entity is required to document a discrete list of Cyber Assets for Low Impact BCS) NRG recommends deleting the quoted portion of the phrase from Section 5 of Attachment 2, number 2: Examples of evidence for Section 5.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures "that document a review of the installed antivirus update level" because it imposes change management requirements where there are not existing NERC requirements	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The requirement allows the entity to have flexibility in creating a plan to best meet the needs of its organization. This includes the production of compliance evidence. The list of example evidence within the measure is not a requirement and is not exhaustive.	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	No

Document Name	
Comment	
ITC Holdings agrees with the comment submitted by NSRF – see below: Please see question 3 for comments concerning “review”. By explaining what the acceptable level of “review” is, the small entity will not be caught in a catch 22. Whereby the “other party” will not state that they meet the attributes of 5.2 and the small entity will have a Low Impact BES Cyber System that cannot be upgraded.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT’s response to NSRF for Question 3.	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Considering the current draft language of the standard, the required evidence can be improved. There is a tradeoff that must be considered between adequate evidence to demonstrate both 1) compliance and assurance that the risk of introduction of malware is mitigated and 2) evidence collection across a large number of sites becoming excessively burdensome. The standard and evidence must be both effective and efficient. The expectations for adequate evidence do not fit the audit style currently being used in compliance monitoring. For example, the CIP Version 5 Evidence Request is clearly written to require often extensive documentation of implementation, whereas the measures documented are inconsistent. The measures should be built to provide an example of evidence that would either meet the current evidence request approach or to clearly communicate the intent of the SDT what appropriate evidence would be. For Measure 5.1, an example of alternative language to clarify audit expectations would be:	

Examples of evidence for Section 5.1 may include, but are not limited to,

1. 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; and

2. Either documentation of an appropriate set of controls that provide a high level of assurance that malware is not present on the Transient Cyber Asset prior to use; or documentation that the Transient Cyber Asset followed the documented method and demonstrates that no identifiable malware is present prior to use.

If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

For Measure 5.3, an example of alternative language that may meet this intent could include:

Examples of evidence for Section 5.3 may include, but are not limited to,

1. Documented process(es) of the method(s) used to detect malicious code; and

2. Either documentation of an appropriate set of controls that provide a high level of assurance that malware is not present on the Removable Media prior to use; or documentation that the Transient Cyber Asset followed the documented method and demonstrates that no identifiable malware is present prior to use.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

The SDT includes examples of evidence it considers valid to meet the requirement. The evidence request is not a product of the SDT. The examples provided in the measures are not intended to be all-inclusive. There are other ways to demonstrate compliance with the requirement that an entity may employ as long as the objective of the requirement is met. The requirement allows the entity to have flexibility in creating a plan to best meet the needs of its organization.

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	No
Document Name	
Comment	
We recommend modifying the first sentence of 5.3.1 to read: “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, including an example of the results.” The original language is confusing, and we believe we should avoid the suggestion of a requirement to capture and retain transactional-level evidence as this would be administratively burdensome.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT asserts that the measure describes the results of scan settings not the scan themselves. Additionally the SDT asserts that the language in a measure is not a requirement. It is up to the entity to determine what would be sufficient evidence of compliance.	
Julie Hall - Entergy - 6	
Answer	No
Document Name	
Comment	
CIP-003-7(i), Attachment 2, Section 5, Part 3 is inconsistent with Part 1. Part 3 states that “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”. Entergy views the documented process(es) and the results of scanning as two separate pieces of evidence. Part 1 identifies the documented process(es) as an acceptable form of evidence with no requirement for scan results for TCA. Part 3 as written implies that all scans results of applicable Removable Media must be maintained in order to provide proper evidence of compliance with CIP-003-7(i), Attachment 1, Section 5.3. This is in stark contrast to the proposed “Supplemental Material” which states that “the SDT does not intend for a Responsible Entity to conduct a review for every single connection of that Removable Media, but implement their	

process(es) in manner that protects all BES Cyber Systems where the Removable Media may be used. The intent is also not to require a log documenting each connection of Removable Media to a BES Cyber Asset." Entergy proposes that CIP-003-7(i), Attachment 2, Section 5, Part 3 be rewritten to more closely mirror Part 1 which identifies the documented process as the evidence item. Specific scan results should be identified as potential additional evidence to support Registered Entities programs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT asserts that the measure describes the results of scan settings not the scan themselves. Additionally the SDT asserts that the language in a measure is not a requirement. It is up to the entity to determine what would be sufficient evidence of compliance.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Seattle City Light agrees with the revisions so far as they go, but finds that they do not address the question of what would be acceptable evidence of the existence of any Low impact Removable Media Asset (based on the proposed definition) in the absence of an explicit list of Low impact BES Cyber Systems and Assets at a facility. As discussed in the definition comment above, Seattle does not have a solution to the problem, which is inherent to the structure of CIP verion 5/6.	
Likes 0	
Dislikes 0	
Response	
While the SDT thanks you for the comment, we decline to make the suggested modification to format. Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required; However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in	

accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Removable Media prior to connecting it to a low impact BES Cyber System(s).	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Same as previous answer.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's response to the previous comment.	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	No
Document Name	
Comment	
We continue to have concerns about how the GTB are factored into Compliance and Enforcement. In some cases it appears that they create "requirements" that must be incorporated into your program; this is inconsistent with prior FERC precedent. On the other hand, it is not clear whether or not you can rely on the GTB in developing your program and ensuring compliance. This concern continues to fail to be addressed by the SDT. With respect to Attachment 1 Section 3, and Attachment 2, Section 3.1, it doesn't make sense to keep referring to physical location when it comes to electronic controls (as previously noted).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	

The G&TB provides SDTs a mechanism to: (i) explain the technical basis for the associated Reliability Standard (and Requirements therein); and (ii) provide technical guidance to help support effective application of the associated Reliability Standard. As provided in the response to draft 2 of CIP-003-7, the requirement language does not prescribe a physical versus logical approach to the implementation. The use of the term "asset" refers to assets identified as containing low impact BES Cyber System(s) pursuant to CIP-002. As described in the G&TB, the Responsible Entity has the flexibility to identify the electronic boundary surrounding the low impact BES Cyber System rather than using a physical boundary.	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
Please see question 3 for comments concerning “review”. By explaining what the acceptable level of “review” is, the small entity will not be caught in a catch 22. Whereby the “other party” will not state that they meet the attributes of 5.2 and the small entity will have a Low Impact BES Cyber System that cannot be upgraded.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT’s response to Question 3.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
There is a concern with the requirement that not only requires an inventory of Transient Cyber Assets and Removable Media but it also requires evidence of chain of custody. The SDT needs to provide clarity on what is required for "evidence of chain of custody".	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment. Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required. However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any TCA or RM prior to connecting it to a low impact BES Cyber System(s). There is no requirement for “evidence of chain of custody."	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Section 5.1 in page 32 to 62: To lighten a obligation of maintaining an inventory of TCA of *Low impact BES Cyber System,* HQP suggest to remove the notion of Trancient asset capability and change the paragraph by “ the Responsible Entity or the vendor may document the method used to mitigate the introduction of malicious code”	
Likes 0	

Dislikes 0	
Response	
Thank you for the comment. Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required. However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any TCA or RM prior to connecting it to a low impact BES Cyber System(s). Compliance with the requirements is the responsibility of the entity being audited.	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Section 5.1 in page 32 to 62: To lighten a obligation of maintaining an inventory of TCA of *Low impact BES Cyber System,* HQP suggest to remove the notion of Transient asset capability and change the paragraph by " the Responsible Entity or the vendor may document the method used to mitigate the introduction of malicious code"	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment. Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required. However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any TCA or RM prior to connecting it to a low impact BES Cyber System(s). Compliance with the requirements is the responsibility of the entity being audited.	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes

Document Name	
Comment	
Tacoma Power supports comments submitted by APPA. Does the Standards Drafting Team intend that any kind of sign-in sheets may be required at assets containing low impact BES Cyber Systems?	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by APPA.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by APPA.	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	

The complexity of the sentences are difficult to read and understand. Suggest revising to bulleted lists. The evidence requirements seem to require an inventory of TCA's and RM. This could be an issue in the same way that a list of BES Cyber Systems has been determined to be an issue.	
Likes 0	
Dislikes 0	
Response	
While the SDT thanks you for the comment, we decline to make the suggested modification to format. Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required. However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Removable Media prior to connecting it to a low impact BES Cyber System(s).	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobby Olsen - Salt River Project - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE noticed the following: • Page 31, Section 1. Cyber Security Awareness; there is an extra "_" that is not needed after the colon symbol. • Page 31, Section 2. Physical Security Controls; there is an extra "_" that is not needed after the colon symbol. • Page 33, Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation; there no period "." at the end of the first continued paragraph.	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. The SDT made the modifications.

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides examples of temporarily connected devices, and strategies to consider in developing the Transient Cyber Asset and Removable Media malicious code mitigation plan(s) at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	No
Document Name	
Comment	
We continue to have concerns about how the GTB are factored into Compliance and Enforcement. In some cases it appears that they create “requirements” that must be incorporated into your program; this is inconsistent with prior FERC precedent. On the other hand, it is not clear whether or not you can rely on the GTB in developing your program and ensuring compliance. This concern continues to fail to be addressed by the SDT. With respect to Attachment 1 Section 3, and Attachment 2, Section 3.1, it doesn't make sense to keep referring to physical location when it comes to electronic controls (as previously noted).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The G&TB provides SDTs a mechanism to: (i) explain the technical basis for the associated Reliability Standard (and Requirements therein); and (ii) provide technical guidance to help support effective application of the associated Reliability Standard. As provided in the response to draft 2 of CIP-003-7, the requirement language does not prescribe a physical versus logical approach to the implementation. The use of the term "asset" refers to assets identified as containing low impact BES Cyber System(s) pursuant to CIP-002. As described in the G&TB, the Responsible Entity has the flexibility to identify the electronic boundary surrounding the low impact BES Cyber System rather than using a physical boundary.	

Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Same as previous answer	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's response to your previous comment.	
Julie Hall - Entergy - 6	
Answer	No
Document Name	
Comment	
Supplemental Material, Requirement R2, Attachment 1, Section 5.1 – Transient Cyber Asset(s) Managed by the Responsible Entity, Paragraph 4 states that if a device will be used to "For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset." This may imply that at least *some* logs might need to be created for connections of TCA to BCA, which is not a requirement stated in the standard for TCAs at low impact BCS, or even for TCAs at Highs and Mediums under CIP-010-2. Additionally, requiring documentation that a TCA was updated before connecting to a BCA removes the device from the on-going program and puts it into on-demand space due to "has been updated before being connected" implying the device is as up to date as possible, even though the on-going process may allow for devices to be updated on a longer regular interval. If the TCA was truly maintained as part of the entitiy's on-going program, no additional log or documentation should be required as the device would be compliant with the standard as written.	

Supplemental Material, Requirement R2, Attachment 1, Section 5.1 – Transient Cyber Asset(s) Managed by the Responsible Entity, Paragraph 4Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System. Periodicity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Requirement R2 is a plan-based requirement, and evidence to demonstrate compliance is based on content in its plan. The requirement allows the entity to have flexibility in creating a plan to best meet the needs of their organization. This may include the specification of update periodicity. Responsible Entities may review the G&TB, RSAW, and corresponding measure(s) for additional information.	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes that for Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems--entities must manage these assets under the program that matches the highest impact level to which they will connect.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This is an example of the why the SDT aligned the language used in the requirements for Transient Cyber Assets used at low impact BES Cyber System(s) and medium/high impact BES Cyber System(s).	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	

Answer	No
Document Name	
Comment	
Considering the current draft language of the standard, the GTB addresses the required points. However, the messages are not clearly, simply, and constructively communicated. While the teams have clearly put a considerable amount of work into ensuring each detail is correct, the overall message in the guidance gets lost. This results in opportunities for multiple different interpretations by various entities and auditors. One possible control is testing the operation of antivirus to test signatures. These should be specifically noted that use of test signatures is not considered identified malware. Section 5.2 (and likely all of the guidance) could be improved if the GTB approach was changed to treat malware protection as a program with specific objectives and a selection of example techniques that may be used to meet these objectives. Further, the guidance should be coordinated with the requirements in development by the Supply Chain SDT.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The obligation specified in the requirement is for entities to implement one or more documented plan(s) for its low impact BES Cyber System(s). The entity has flexibility to determine what methods to include in its plan so long as they meet the security objective to mitigate the risk of the introduction of malicious code into the BES Cyber System through the use of Transient Cyber Assets or Removable Media.	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	No
Document Name	
Comment	

ITC does not agree with the proposed modification in regards to guidance provided for awareness training. The revised guidance states "The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel". This statement is ambiguous and leaves the interpretation as to whether or not tracking of reception of awareness training is actually required to maintain compliance. The specific and direct language of "Responsible Entity is not required" should be retained, to reduce confusion and ambiguity as to if this is required for compliance and not left to the disposition of individual auditors. ITC recommends that this specific change be struck and the original language to stand. All other changes are acceptable.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT made the change to reflect that the G&TB does not prescribe what is or is not required to demonstrate compliance.	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
NRG recommends correction of grammatical / spelling error: on page 57 of 62 of the Guidelines and Technical basis section for requirement 2. • If a Responsible Entity chooses *to use* methods that mitigate the introduction of malicious code other than those listed, it should *document* ***at*** how the other method(s) meet the mitigation of the introduction of malicious code objective. Pertaining to project 2016-02, NRG recommends that the Low Impact requirements should be incorporated into the existing CIP standards using applicability tables because this would remove inconsistencies and confusion between L/M/H and provide more efficiency within the industry. For example, applied CIP-010-2 Attachment 1 for TCA and Removable Media requirements, with the exception of the authorized user or machine lists.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has made the suggested changes. While the SDT appreciates the comments regarding the placement of the low impact requirements, we decided to retain the current CIP-003 plan structure due to a majority of stakeholder support.	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation appreciates the Standards Drafting Team's consideration of prior recommendations. Reclamation agrees with the changes and has the following comment: In the redline version of the Guidelines and Technical Basis, some typographical errors include: • The spelling of "Responsible Entities" on the sixth line of page 55. • A duplicate paragraph at the bottom of page 56 and the top of page 57. • The spelling of "to use" and "document" in the third bullet of page 57. • The word "is" at the beginning of a sentence on the third line from the bottom of page 57.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT made the suggested modification.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The information in the GTB section does not appear to be consistent with the information in Requirement R2. Our interpretation of Requirement R2 suggests that there is not enough clarity in the Requirement to differentiate whether the focus is solely on CIP-002 and its attachment 1 or is the focus more on CIP-003-7(i) and its Attachment 1. We suggest adding clarity to the Requirement and/or the GTB to ensure that there is no confusion as to the Requirement's intent as well as what an audit team's interpretation of the performance of an entity during the auditing process.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Where Attachment 1 or Attachment 2 is specified within the standard without explicit reference to another standard, the attachment pertains to the standard wherein the reference was made. No change made.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes. To avoid confusion with CIP-010 R1 requirements, we suggest the removal of "change management process" in the prior sentence.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that there is no obligation for entities to implement a change management process for low impact BES Cyber System(s), although entities may have such processes. The G&TB does not and cannot introduce any obligations that are not specified in the requirement language.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Seattle City Light appreciates the extra efforts of the Standard Drafting Team to provide such guidance and technical information. However, Seattle asks that Guidelines and Technical Basis information be provided for new Section 1.2.6 as well. This guidance would	

address how a CIP Exceptional Circumstance is considered when applied against a requirement that does not explicitly mention that a CIP Exceptional Circumstance applies.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT agrees that providing guidance on the low impact policy is beneficial and has made such modifications to the G&TB. However, the SDT notes that - unless explicitly stated - CEC does not apply.	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
1) The guidance should be coordinated with the Supply Chain SDT. 2) The GTB language that states: “Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.” is to prescriptive. Recommend that the “are to” be changed to “may”. The use of prescriptive language like “should” and “are to” should be used on a very limited basis if not removed entirely. Guidance should be shifted to a programmatic approach.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Project 2016-02 Modifications to CIP Standards SDT is coordinating with the Supply Chain SDT as necessary.	

The SDT updated the G&TB to more closely align with the requirement language. The intent is to reiterate the need to document and implement the plan as specified in the requirement, not to infer other obligations in the G&TB.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by APPA.	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Page 56 of the Guidelines and Technical Basis includes a section titled "Vulnerability Mitigation"; however, Requirement R2, Attachment 1, Section 5 is titled "…Risk Mitigation". AZPS requests clarification and consistency regarding the terms vulnerability and risk as one term is more subjective than the other.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated this section of the G&TB to more closely align with the language used in Attachment 1.	

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by APPA.	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
No comments for section 5.	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
None.	

Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG	
Answer	Yes
Document Name	
Comment	
Two comments. First, recommend changing “should” to “may” in this paragraph To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.1 Procurement language may unify the other party’s and entity’s actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party’s support. Entities should consider the “General Cybersecurity Procurement Language” and “The Supplier’s Life Cycle Security Program” when drafting Master Service Agreements, Contracts, and the CIP program processes and controls. Second, recommend updating 5.3 from “If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System.“ to “If malicious code is discovered, it must be removed or mitigated prior to connection to a BES Cyber Asset or BES Cyber Systems in order to prevent the malicious code from being introduced into the BES Cyber Asset or BES Cyber System.“	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments. The SDT modified the G&TB accordingly.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
The guidance should be coordinated with the Supply Chain SDT.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2016-02 Modifications to CIP Standards SDT is coordinating with the Supply Chain SDT as necessary.	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobby Olsen - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE noticed the following:

- Page 56, Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity states, "*For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect*." Since this concept is the same as described in the Guidelines and Technical Basis of CIP-005-5, Texas Re suggests that the SDT use the same "high water mark" language found in the Guidelines and Technical basis of CIP-005-5 to stay consistent.
- Page 57, Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity states, "*The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset*." Texas RE considers keeping a list of BES Cyber Assets as best practice and this language discourages it. Texas RE encourages entities to have an inventory of their low impact BES Cyber Systems.
- Page 57, Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity states, "*If a Responsible Entity chooses touse methods….*" There should be a space between "touse".

Likes 0	
Dislikes 0	
Response	

Thank you for your comments.

The SDT asserts that the language is sufficiently clear in the G&TB to describe the necessary treatment of Transient Cyber Assets. Requirement R2 is a plan-based requirement, and evidence to demonstrate compliance is based on the content in the entity's plan(s). While an entity may comply with the requirement by creating an inventory, the G&TB is accurate in conveying that the intent of the SDT was not to create such an obligation. The SDT made the modification.	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	
Document Name	
Comment	
1) The guidance should be coordinated with the Supply Chain SDT. 2) The GTB language that states: "Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed." is to prescriptive. Recommend that the "are to" be changed to "may". The use of prescriptive language like "should" and "are to" should be used on a very limited basis if not removed entirely. Guidance should be shifted to a programmatic approach.	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. The Project 2016-02 Modifications to CIP Standards SDT is coordinating with the Supply Chain SDT as necessary. The SDT updated the G&TB to more closely align with the requirement language. The intent is to reiterate the need to document and implement the plan as specified in the requirement, not to infer other obligations in the G&TB.

6. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline. Were the CEC language is explicitly stated, entities need not
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	
Comment	
We suggest the drafting team include the approval of the RSAW into the Implementation Plan as this is a significant and related document.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The RSAW is not a product of the SDT.	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	

Comment	
Pertaining to project 2016-02, CIP-003-7(i), it doesn't appear that the implementation plan accounts for additional time to implement 1.2.5 and 1.2.6. NRG recommends that the implementation plan allow for 18 months implementation time of 1.2.5 and 1.2.6. (the same implementation time as other requirements)	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The implementation plan specifies that CIP-003-7(i) will become effective 18 months following applicable regulatory approval. This is inclusive of the modifications to Requirement R1.	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	No
Document Name	

Comment
ITC Holdings agrees with the comments compiled by the EEI CIP Standards subgroup– see below: SUMMARY: CIP-003-6, Requirement R2, Attachment 1, sections 2 and 3 have been approved (under the Order No. 822 implementation plan) to be effective on September 1, 2018. However, in Order No. 822, the Commission ordered NERC (within 1 year) to provide clarity regarding the LERC (Low Impact External Routable Connectivity) definition, specifically ambiguity surrounding the term "direct" used in the definition. When the SDT set out to modify the definition they found that it was more appropriate to modify the requirement language to address the ambiguity. The modified standard (version 7) is expected to be filed with FERC by March 31, 2017. CIP-003-6, Requirement R2, Attachment 1, sections 2 and 3 is effective September 1, 2018 and version 7, if FERC approves, will be effective 18 months from FERC's approval, so doing rough math (March 31, 2017 NERC filing of version 7, August 2017 NOPR--assuming

~5 months FERC review, February 2018 FERC approval--assuming 60 day notice and comment, and 3 month FERC review): version 7 would become effective around August 2019, basically a year after Version 6 (the time it took NERC to make the modification).

RATIONALE:

Reasons for supporting a change to the implementation plan: 1) retiring the implementation of CIP-003-6, attachment 1, sections 2 and 3; 2) synching up the implementation the low impact BES Cyber System modifications (attachment 1, sections 2, 3, and 5); and 3) giving entities 18 months to implement these sections:

1. Companies will not have certainty regarding CIP-003-6 implementation until February 2018, but will have to move forward on version 6 to make the Sept. 2018 compliance deadline or accept the compliance risk by not implementing version 6.
2. According to the Commission (Order No. 822), the CIP-003-6 modification "is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition." As a result, implementation of CIP-003-6 without the modification doesn't make much sense in light of the ambiguity identified by the Commission.
3. Low impact BES Cyber Systems (LIBCS) have a low impact to the BES compared to medium and high impact BES Cyber Systems.
4. LIBICS number in the tens of thousands systems; it will take time to carefully implement the new CIP-003 requirements. Implementing CIP-003-6 LERC, CIP-003-7 LERC, and then CIP-003-7 TCA in three steps will strain resources for systems with low impact to the BES. It would be more efficient to implement just the CIP-003-7 LERC and TCA modifications at the same time.
5. Change management at this scale, will also be more effective if done all at once, which will help reduce the potential spike in audit violations.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

The SDT agrees that it is important to align the initial implementation of Sections 2, 3 and 5 of Attachment 1. The effective dates or phased-in compliance dates within the CIP-003-6 Implementation Plan, remain in effect except that the compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7.

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
While achievable in 18 calendar months, the standard needs significant improvement before a yes vote on the implementation.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to the subject comments.	
Julie Hall - Entergy - 6	
Answer	No
Document Name	
Comment	
Entergy cannot agree with the Implementation Plan timeline given the standard as written, and the concerns discussed in the comments submitted above. Until clarity is given regarding the scope and evidentiary requirements necessary to achieve compliance, Entergy cannot support the short implementation timeline proposed as the feasibility of implementing controls and evidenciary requirements to meet the standard as currently drafted in that small timeframe for an Entity as large as Entergy is miniscule.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT asserts that the 18 month implementation period is sufficient for entities to implement the standards.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
The majority of actions necessitating the timeframe proposed in the Implementation Plan modifications involve identifying and implementing the physical, electronic, and TCA/RM controls necessary for over 1200 assets containing Low Impact BES Cyber Systems, as well as training a massive amount of personnel on meeting and maintaining compliance with these new Standard requirements. Although the requirements themselves may be less rigid than those for Highs and Mediums, the proposed implementation timeframe is required from a volume standpoint, as well as from a risk-based standpoint so as not to divert attention and resources away from meeting and maintaining compliance on all of the other High and Medium risk assets	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes

Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
We strongly support the Implementation Plan, which seeks to replace compliance with CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 with compliance with CIP-003-7(i) (and CIP-003-7) such that only one implementation is required for the LIBICS modifications, 18 months from FERC approval. Our members agree with the SDT's approach and offer further explanations as to the importance of this implementation plan: 1. For CIP-003 alone, EEI members are looking at 3 implementation phases for a very large group of disaggregate assets (substations with variations among systems, types, shared footprints and components as well as generating stations that are extremely complex with many different systems and manufacturers involved). LIBCS number in the tens of thousands of systems; it will take time to carefully implement the new CIP-003 requirements. Implementing CIP-003-6 LERC, CIP-003-7 LERC, and then CIP-003-7 TCA in three steps will strain resources for systems with low impact to the BES. 2. Change management at this scale, will also be more effective if done all at once, which will help reduce the potential spike in audit violations. When we say more effective, we really mean doing it right for security and reliability. Training on one change for CIP-003-6 and then training again for CIP-003-7 will create confusion for field forces. Having one date to train on this culture change management would be more effective when an entity needs to train 250 plus field and engineering people regarding 550 or more low impact BES Cyber	

Systems. If field people are confused, they will make or may be prone to make mistakes due to confusion or rapidly changing expectations. Potential violations will not protect against security threats or reliability issues. 3. Shared facilities create another implementation issue. For example, an EEI member has approximately half of their low impact substations owned by third parties, shared facilities. To make each of the section 2 and 3 changes, they will have to physically go to each substation, which are owned by different entities and as a result are all different. As a result, the approaches they take at each facility must be different, which is also a good thing in the security world. Eighteen months is necessary to make these changes. 4. The revised CIP-003-7 language including retirement of the LERC definition improves the clarity of the requirements. However, the revisions represent a change in assessment approach and will precipitate a new analysis of which locations will be in scope for section 3. The LERC definition provided a filter by the use of the word 'direct' that could be applied when determining which locations were in scope. The retirement of LERC removed that filter. The new language replacing the LERC definition established new assessment criteria and applies it regardless of direct or indirect connectivity. The change to LERC requires Responsible Entities to perform a new analysis of each of their locations. Applying the CIP-003-7 requirements means that entities must walk down each location in scope to determine the specific configurations (physical and electronic) that exist at the location. These walk downs are currently underway to apply a -6 implementation focused on the definition of LERC from CIP-003-6. The scope of analysis will change under CIP-003-7, so that all locations must be assessed for connectivity and then assessed against the new criteria.	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
No comments for section 6.	
Likes 0	
Dislikes 0	

Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy agrees with EEI's comments regarding the implementation plan for the Low Impact BES Cyber System modifications.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by EEI.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by APPA.	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	

Comment	
Duke Energy agrees with the comments submitted by EEI regarding the proposed Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by EEI.	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Companies with a large number of low impact assets will need this time to educate users about handling TCAs and Removable Media. These assets are categorized as low impact because they inherently have a low ability to negatively impact the Bulk Electric System. We do not want to focus our resources on rolling out this education at the expense of efforts that mitigate risks to assets that inherently have a greater ability to negatively impact the Bulk Electric System.	

During the 18-month implementation plan, we will design the overall processes taking into consideration differences between different plant types (gas, lignite, combustion turbine and combined cycle). We will roll out that program to a single pilot plant to identify lessons learned and improve the experience as we onboard subsequent plants. We anticipate spending 3-5 months to design the processes and pilot the program. The remaining months will be spent rolling out to our fleet (40 units at 15 plants). The 18-month implementation plan is appropriate as it allows us to carefully and thoughtfully assign resources to most effectively and efficiently mitigate cyber risk.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobby Olsen - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not necessarily object to the SDT's proposed 12-month implementation period. However, Texas RE respectfully requests that the SDT provide a basis for its decision to adopt such a 12-month compliance window, including any data it considered in determining that this was an appropriate window for affected entities to meet their compliance obligations under the revised Standards.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

7. If you have additional comments on the proposed revisions to address the FERC directive regarding TCAs for low impact BES Cyber Systems that you have not provided in response to the questions above, please provide them here.
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF
Answer
Document Name
Comment
Small entities will not be able to go up against a vendor (i. e. Micro Soft in size) and request to review their most current protections to comply with section 5.2. The above clarity will assure we meet the attributes of 5.2. The NSRF does not wish for CIP-003-7(i) to be the number one non compliance Standard going forward in NERC, similar to CIP-007-6.
Likes 0
Dislikes 0
Response
Thank you for your comment. Please see the SDT's response to Question 4.
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino
Answer
Document Name
Comment
Entities are increasing their use of malicious code mitigation using tools such as Cylance, which does not rely on signatures or updates. The measures should consider these tools and provide examples of evidence that will prove compliance.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT contends that your concern is addressed in the last bullet of Attachment 1, Section 5, Part 5.2 that allows entities the flexibility to use “other method(s) to mitigate the introduction of malicious code.” Measures provide examples of evidence and are not intended to be comprehensive lists. Each entity has to decide and provide whatever evidence it determines best demonstrates compliance with any requirement.	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	
Document Name	
Comment	
none	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	
Document Name	
Comment	

Dominion recommends that the first VSL conditional statement for Requirement 1 Part 1.2 (page 14 of 62 of draft 1 of CIP-003-7(i)) be consistent with the prior version of CIP-003 and read as follows: Lower VSL: The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two or fewer of the six topics required by R1. (R1.2) Moderate VSL: The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the six topics required by R1. (R1.2) High VSL: The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four of the six topics required by R1. (R1.2) Severe VSL: The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address five or more of the six topics required by R1. (R1.2) The revised VSLs accurately reflect the actual severity when a failure to address the appropriate topics occurs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT notes that the current VSL structure is in alignment with CIP-003-6, CIP-003-7, and the informal posting of CIP-003-7(i).	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
Seattle City Light has additional concerns that led it to vote NO for this ballot. One concern is about new sub-part 1.2.6, which introduces CIP Expectional Circumstances to Low impact facilities. The other concern is about seeming errors in the Violation Severity Level (VSL) tables for some of the new parts and sections introduced in CIP-003-7(i).	

Regarding sub-part 1.2.6, Seattle supports the concept of allowing CIP Exception Circumstances for Low impact facilities and related requirements, and find this idea highly sensible and reasonable. Seattle is concerned, however, that the change appeared without notice or discussion in the present draft of CIP-003-7(i), and that the application of CIP Expectional Circumstances for Lows is not at all defined. In particular, other Standards, parts, and sub-parts of CIP version 5/6 explicitly identify where CIP Exceptional Circumstances are allowed. This explicit mention creates the presumption that CIP Exceptional Circumstances are allowed only for said Standards, parts, or sub-parts; some auditors have stated as such. Seattle is aware that an drafting team effort is planned to address inconsistencies in the existing application of CIP Exceptional Circumstances, and finds it premature to expand the use of CIP Exceptional Circumstances in a way that introduces even more uncertainty—how are they applied to Lows where no existing Low Standard mentions that CIP Expectional Circumstances are allowed—before the existing issues are addressed. That the concept was introduced without discussion or technical guidance language only heightens our concern. As a possible corrective, Seattle recommends that the Part R2 of CIP-003-7(i) be modified as follows (BOLD text is new):

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall, EXCEPT FOR CIP EXCEPTIONAL CIRCUMSTANCES, implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.

Regarding the VSL tables, Seattle does not understand the difference among the Lower, Moderate, and High VSLs for failure to perform some or all of the activities according for Requirement R2, Attachment 1, Section 5.1. For Transient Cyber Assets, the Lower VSL states:

The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2)

The applicable Moderate VSL states:

The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2)

And the applicable High VSL reads:

The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) Seattle does not understand the difference among the three items, given that the failure to manage according to plan (the Lower VSL) means that introduction of mitigation code is not documented (the Moderate VSL) and/or mitigated (High VSL); there are not other applicable activities to fail. As such, Seattle recommends these be consolidated into a single VSL at the Moderate (or perhaps High) level. Finally, Seattle also finds confusing the wording in the Lower VSL for Removable Media. For Transient Cyber Assets this VSL states: The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) Seattle does not understand how an entity can ever meet the Lower VSL for Removable Media, in that to do so it must "document its plan(s) for…Removable Media but fail to document the Removable Media section(s) according to Requirement 2." As best as we understand, the Removable Media Plans are the Removable Media sections of Requirement 2, so the statement appears to be in error. As a corrective, Seattle suggests that the Lower VSL entry for Removable Media be modified to mirror that of Transient Cyber Assets, and thus read (BOLD indicates where "Removable Media" was substituted for Transient Cyber Asset): The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its REMOVABLE MEDIA according to Requirement R2, Attachment 1, Section 5.1. (R2)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Due to the requirement to perform actions at the time of use of a TCA or RM, an entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation. The other sections under Attachment 1 do not have the same timing aspects as Section 5. The SDT will be seeking industry feedback on the applicability of CEC to other requirements and parts. Requirement 1.2.6 was added to ensure a policy for CEC in the use of TCA and RM. Requirement 1.2.6 was	

added to ensure a policy for CEC in the use of TCA and RM. Guidance was added for policy section 1.2.6 on declaring and responding to CEC. The difference related to TCAs are as follows, the Lower VSL addresses the documentation and management aspects of the requirement. The entity documented its plan but did not follow the plan in managing its TCAs under Section 5.1. The Moderate VSL addresses the situation where the entity documented their plan, mitigated discovered malicious code, but failed to document the mitigation. The High VSL addresses where the entity failed to mitigate the introduction of malicious code. Regarding the Lower VSL for Removable Media, the SDT has revised the VSL to state: The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
BPA respectfully suggests spellchecking the redline before finalizing. For example: Page 33: Entiteis Page 57: Transiet	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	

Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	
Document Name	
Comment	
1) The word “and” should be added at the end of R1.2.5 2) This comment form did not reference the addition of CIP Exceptional Circumstances as Requirement R1.2.6 and the inclusion of the phrase “except under CIP Exceptional Circumstances” in Attachment 1, Section 5. The “except under CIP Exceptional Circumstances” phrase should also be addressed in Attachment 1 Sections 2 and 3. Not addressing CEC in Sections 2 and 3 may result in a “no” vote for on future ballot of this standard. 3) A Section 6 under Attachment 2 is needed to explain how the CIP Exceptional Circumstance is to be used so you can put it into your policy/plan accordingly.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	

The word "and" was added to Requirement R1, Part 1.2.5. Due to the requirement to perform actions at the time of use of a TCA or RM, an entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation. The other sections under Attachment 1 do not have the same timing aspects as Section 5. The SDT will be seeking industry feedback on the applicability of CEC to other requirements and parts. Requirement 1.2.6 was added to ensure a policy for CEC in the use of TCA and RM. Guidance was added for policy section 1.2.6 on declaring and responding to CEC.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by APPA.	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	
Document Name	
Comment	
ITC Holdings agrees with the comment submitted by NSRF – see below: Small entities will not be able to go up against a vendor (i. e. Micro Soft in size) and request to review their most current protections to comply with section 5.2. The above clarity will assure we meet the attributes of 5.2. The NSRF does not wish for CIP-003-7(i) to be the number one non compliance Standard going forward in NERC, similar to CIP-007-6.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to Question 4.	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	

Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators	
Answer	
Document Name	
Comment	
1. The inclusion of CIP Exceptional Circumstance for lows adds additional compliance burden above and beyond the FERC Directives. This will require Cyber Security Policy revisions, training and increase audit risk for lows who have not seen any addtioal risks to the BES to require CIP Exceptional Circumstances as part of their CIP cyber Security Program. 2. If a low impact entity connects an identified 30-day TCA beyond the thirty days, what is the classification of the asset? If this was a high or medium impact entity, the TCA would be classified as a Protected Cyber Asset (PCA). However, PCAs are not applicable to low impact entities, as a low impact's TCA would not be classified as a BES Cyber Asset that could impact the BES within 15 minutes. Would the low impact entity who failed to connect the TCA within the thirty day timeframe have to self-report the TCA to Regional Entities? If so, this would impose a greater violation risk for lows than for high and medium impact entities. 3. We thank the SDT for this opportunity to provide comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. 1. An entity is not obligated to use TCAs or RM. The inclusion of CEC for lows was added due to the requirement to perform actions at the time of use of a TCA or RM. An entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation. 2. The TCA connected for more than 30 days could be considered a BES Cyber System or a non-BES Cyber System, depending on the facts and circumstances. The handling of this situation could be addressed within the entity's plan.	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	

Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by APPA.	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
No comments for section 7.	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	
Document Name	
Comment	
Some typos: P 55: 'entiteis' P 70 of 75: “touse”; “. is the SDT”; “toTransiet Cyber Assets”	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT made the modifications.	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	
Document Name	
Comment	
Xcel Energy supports the comments of the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by EEI.	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	
Document Name	
Comment	
The CIP Exceptional Circumstance concept does not belong with the Low Impact requirements. The purpose of CIP-007-3i was to define and create requirements for Transient Cyber Assets and Removable Media. The need for Exceptional Circumstances for High and Medium is because the Standard mandates a PRA for unescorted access. Even with Exceptional Circumstances you have to report a violation because of the externally mandated PRA. In the case of Low Impact, the entity writes the requirements for access. Most departments responsible for physical security automatically allow the entrance of Emergency Personnel and Police if there is an alarm or	

911 call. This could be written into each Responsible Entity's Low Impact Cyber Security Policy (CIP-003 R1.2) but that doesn't seem to support BES Reliability.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Due to the requirement to perform actions at the time of use of a TCA or RM, an entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation. The other sections under Attachment 1 do not have the same timing aspects as Section 5. The SDT will be seeking industry feedback on the applicability of CEC to other requirements and parts.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE notes some possible issues with the proposed Violation Severity Levels associated with the proposed additions to CIP-003, Attachment 1. First, the second proposed "Lower VSL" provides that "[t]he Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to Requirement R2, Attachment 1, Section 5.3." Although it is possible to read the VSL language as referring first to general documentation for TCAs and Removable Media and then to the two specific Removable Media elements identified in Section 5.3, this connection could be made clearer. One approach would be revise the Lower VSL to read "The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the use of method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or mitigation of the threat of detected malicious code on Removable Media prior to connecting Removable Media to a low impact BES Cyber System." Second, and related to the first issue above, the initial additional "Moderate VSL" provides that the Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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." (emphasis	

added). However, Section 5.3 applies to Removable Media and not TCAs. As such, the reference here seems inappropriate and potentially conflicts with the "Low VSL" for documentation of Removable Media mitigation described above. Texas RE recommends that the SDT either eliminate the reference to Section 5.3 here, or develop a new "Moderate VSL" applicable to the mitigation requirements for Removable Media in Section 5.3. The Standard Drafting Team should further ensure that this approach is consistent with the "Low VSL" for Removable Media documentation as well. Finally, while Texas RE does not necessarily object to the general VSL assignments at this time, Texas RE respectfully requests that the SDT provide a basis for its decisions to assign VSL categories to the various elements. In particular, Texas RE would like to understand the SDT's decision to assign "Low" and "Moderate" VSL categories to Removable Media and "Moderate" and "High" VSL categories to Transient Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. 1. Regarding the Lower VSL for Removable Media, the SDT revised the VSL to state: The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) 2. First VSL related to Requirement R2, Attachment 1, Section 5.3 under Moderate addresses the situation where the entity documented their plan, mitigated discovered malicious code, but failed to document the mitigation. The second VSL related to Requirement R2, Attachment 1, Section 5.3 addresses the situation where the entity failed to implement the Removable Media sections.	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	
Document Name	

Comment
1) The word “and” should be added at the end of R1.2.5 2) This comment form did not reference the addition of CIP Exceptional Circumstances as Requirement R1.2.6 and the inclusion of the phrase “except under CIP Exceptional Circumstances” in Attachment 1, Section 5. The “except under CIP Exceptional Circumstances” phrase should also be addressed in Attachment 1 Sections 2 and 3. Not addressing CEC in Sections 2 and 3 may result in a “no” vote for on future ballot of this standard. 3) A Section 6 under Attachment 2 is needed to explain how the CIP Exceptional Circumstance is to be used so you can put it into your policy/plan accordingly.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The word "and" was added to Requirement R1, Part 1.2.5. Due to the requirement to perform actions at the time of use of a TCA or RM, an entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation. The other sections under Attachment 1 do not have the same timing aspects as Section 5. The SDT will be seeking industry feedback on the applicability of CEC to other requirements and parts. Requirement 1.2.6 was added to ensure a policy for CEC in the use of TCA and RM. Guidance was added for policy section 1.2.6 on declaring and responding to CEC.

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	
Document Name	

Comment
N/A

Likes 0	

Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	
Document Name	
Comment	
To address the changes to the RSAW provided on January 20th Under the Note to Auditor section, Attachment 1, Section 3: Bullet 1: Recommended to state that "the devices used to control electronic access" can be documented at a representative level. The standard (Attachment 1, Section 3, Bullet 1) under examples of evidence state that documentation can be "at each asset or group of assets containing low impact BES Cyber Systems" level and can be representative diagrams, meaning a list of devices at each asset is not required under the standard and puts additional documentation burden on the Entity as currently worded in the RSAW. Bullet 2: Recommended to document necessary inbound and outbound routable protocols communications at a standard level versus at each asset (e.g. document SCADA communications as necessary inbound and outbound for the Entities entire system, rather than having to document at each asset) for same reason as our comment for Bullet 1. Bullet 3 and 4: Recommended to document that the electronic access controls can be provided at a standard level (e.g. standard configurations) which would apply to the standard devices, versus providing per asset.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT provided your comments regarding the RSAW to NERC staff for review.	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	

Answer	
Document Name	
Comment	
PacifiCorp supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to comments submitted by EEI.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	
Document Name	
Comment	
1) This comment form did not reference the addition of CIP Exceptional Circumstances as Requirement R1.2.6 and the inclusion of the phrase "except under CIP Exceptional Circumstances" in Attachment 1, Section 5. The "except under CIP Exceptional Circumstances" phrase should also be addressed in Attachment 1 Sections 2 and 3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Due to the requirement to perform actions at the time of use of a TCA or RM, an entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation. The other sections under Attachment 1 do not have the same timing aspects as Section 5. The SDT will be seeking industry feedback on the applicability of CEC to other requirements and parts.	

Additional comments received from American Public Power Association

1. Definition: The SDT revised the definition of Transient Cyber Asset such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes: X

   No:

   Comments:
   Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Transient Cyber Asset definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.

   Response:
   Thank you for your comment.

   The SDT included the referenced language in the definitions to specifically address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems. No additional guidance is required.

2. Definition: The SDT revised the definition of Removable Media such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes: X

   No:

   Comments:
   Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Removable Media definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.

Response:
Thank you for your comment.

The SDT included the referenced language in the definitions to specifically address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems. No additional guidance is required.

3. Requirement R2: The SDT revised CIP-003-7(i), Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to mitigate the risk of propagation of malware from transient devices. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes: X

   No:

   Comments:
   1) The bulleted list creates requirements that are too prescriptive. Use alternative language for Section 5.1 and 5.2 to remove the bullet points (because they may be used against you in some fashion in the future), and re-write the requirements. The bullet points should go into the GTB section so that there is less chance for a misinterpretation or reinterpretation that would require the implementation of more than one of the bulleted point in order to meet compliance.

   2) As written, the requirements listed for TCAs in CIP-003-7(i) for Low Impact assets is a subset of the requirements for high and medium impact included in CIP-010-2 R4. If this list remains the same or if changed the GTB section should include a statement that low impact requirements are a subset of those for High and Medium.

   Response:
   Thank you for your comments.

   The use of the bulleted list is consistent with other currently approved standards. The SDT's intention in using the bulleted list is to provide options to satisfy the parent statement, and the SDT purposely included the ability for the Responsible Entity to use other protection methods, rather than those listed, that more adequately fit the entity's environment.

The relationship between highs, mediums, and lows is addressed in Attachment 1 to allow entities to utilize a single program for all impact levels.

4. Attachment 2: The SDT revised the evidential language of CIP-003-7(i), Attachment 2, Section 5 to make the Measures consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

   Yes: X

   No:

   Comments:
   The complexity of the sentences are difficult to read and understand. Suggest revising to bulleted lists. The evidence requirements seem to require an inventory of TCA's and Removable Media. This could be a significant burdent on registered entities in the same way that a list of BES Cyber Systems has been determined to be an issue.

   Response:
   Thank you for your comment.

   While the SDT thanks you for the comment, we decline to make the suggested modification to the format. Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required. However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Removable Media prior to connecting it to a low impact BES Cyber System(s).

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides examples of temporarily connected devices, and strategies to consider in developing the Transient Cyber Asset and Removable Media malicious code mitigation plan(s) at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

   Yes: X

   No:

Comments:
1) The guidance should be coordinated with the Supply Chain SDT.

2) The GTB language that states: "Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed." is too prescriptive. Recommend that the "are to" be changed to "may". The use of prescriptive language like "should" and "are to" should be used on a very limited basis if not removed entirely. Guidance should be shifted to a programmatic approach.

Response:
Thank you for your comments.

The Project 2016-02 Modifications to CIP Standards SDT is coordinating with the Supply Chain SDT as necessary.

The SDT updated the G&TB to more closely align with the requirement language. The intent is to reiterate the need to document and implement the plan as specified in the requirement, not to infer other obligations in the G&TB.

6. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

   Yes: X

   No:

   Comments: None

7. If you have additional comments on the proposed revisions to address the FERC directive regarding TCAs for low impact BES Cyber Systems that you have **not** provided in response to the questions above, please provide them here.

Comments:

1) The word “and” should be added at the end of R1.2.5

2) This comment form did not reference the addition of CIP Exceptional Circumstances in Requirement R1.2.6 and the inclusion of the phrase “except under CIP Exceptional Circumstances” in Attachment 1, Section 5. The “except under CIP Exceptional Circumstances” phrase should also be addressed in Attachment 1 Sections 2 and 3. Not addressing CIP Exceptional Circumstances in Sections 2 and 3 may result in a “no” vote on future ballot of this standard.

3) A Section 6 under Attachment 2 is needed to explain how the CIP Exceptional Circumstance is to be used so you can put it into your policy/plan accordingly.

Response:

Thank you for your comments.

The word "and" was added to Requirement R1.2.5.

Due to the requirement to perform actions at the time of use of a TCA or RM, an entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation. The other sections under Attachment 1 do not have the same timing aspects as Section 5. The SDT will be seeking industry feedback on the applicability of CEC to other requirements and parts. Requirement 1.2.6 was added to ensure a policy for CEC in the use of TCA and RM. Guidance was added for policy section 1.2.6 on declaring and responding to CEC.

End of Report

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.

Description of Current Draft

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions to be incorporated into the Glossary of Terms Used in NERC Reliability Standards. In addition to approving the seven CIP Reliability Standards, the Commission, directed NERC to, among other things,: (1) "…develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems…", and (2) modify the definition of LERC.

In response to these directives, NERC first modified Reliability Standard CIP-003-6 to address the LERC directive which has a regulatory deadline of March 31, 2017 for filing with the Commission. The revisions associated with the LERC directive were developed and posted for comment and ballot in July 2016 in draft Reliability Standard CIP-003-7. The revisions were not approved by stakeholders and based on the feedback received, the drafting team revised its approach and posted the revisions for an additional comment period and ballot. CIP-003-7 passed the additional ballot that ended on December 5, 2016.

For the transient device directive, NERC initially posted draft revisions for an informal comment period from November 1-18, 2016. This draft of Reliability Standard CIP-003-7(i) incorporates the proposed TCA language, as modified based on stakeholder comment, with the recently passed LERC revisions. The intent of this approach is to allow entities time to efficiently plan and implement the required modifications for low impact BES Cyber Systems. The Standard Drafting Team (SDT) approach to address the transient device directive is summarized below.

The SDT revised Attachment 1 of CIP-003-7 to include requirements that mitigate the risk to the BES of malware propagation from transient devices to low impact BES Cyber Systems. Attachment 1 contains and outlines the required sections of a Responsible Entity's cyber security plan(s) for its low impact BES Cyber Systems per Requirement R2. Previously, cyber security plan(s) were required to address four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. In keeping with the stakeholder approved approach to incorporate into one standard all the requirements applicable to assets containing low impact BES Cyber Systems, the SDT expanded CIP-003-7 Attachment 1 to include a fifth area: "Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation." Requiring the Responsible Entity to develop and implement these plans will provide higher assurance against the propagation of malware from transient devices.

In addition, the SDT determined it was necessary to revise the definitions of a Transient Cyber Asset (TCA) and Removable Media to ensure applicability of security controls and provide additional clarity. As well, the revised definitions accommodate use of the terms for all impact

levels: high, medium, and low. This is important for those entities that may opt to deploy one program to manage TCAs and Removable Media across multiple impact level assets.

The proposed revised definition of a Transient Cyber Asset (TCA) is:

A Cyber Asset that is:

1. *capable of transmitting or transferring executable code,*
2. *not included in a BES Cyber System,*
3. *not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and*
4. *directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:*
    - *BES Cyber Asset,*
    - *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
    - *PCA associated with high or medium impact BES Cyber Systems.*

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

The proposed revised definition of Removable Media is:

Storage media that:

1. *are not Cyber Assets,*
2. *are capable of transferring executable code,*
3. *can be used to store, copy, move, or access data, and*
4. *are directly connected for 30 consecutive calendar days or less to a:*
    - *BES Cyber Asset,*
    - *network within an Electronic Service Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
    - *Protected Cyber Asset associated with high or medium impact BES Cyber Systems.*

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

As proposed, Section 5 of Attachment 1 of CIP-003-7(i) mandates that entities have malware protection on TCAs (both entity and vendor-managed) and for Removable Media. The SDT proposes that it is necessary to distinguish between the specific protections for: (i) TCAs managed by the Responsible Entity, (ii) TCAs managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media.

For TCAs managed by the Responsible Entity, Section 5 requires the Responsible Entity to use one or a combination of the following to mitigate the introduction of malicious code: antivirus software, application whitelisting, or some other method. The SDT recognizes that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices (i.e., manage in an ongoing manner) while others have a checklist for transient devices prior to connecting them to a BES Cyber System (i.e., manage in an on-demand manner). The SDT acknowledges that both methods are effective and Section 5 permits either form of management. Because of the higher frequency in which these entity-managed devices are used, the controls required for these devices are more specific.

For Transient Cyber Assets managed by a party other than the Responsible Entity, Section 5 requires the Responsible Entity to review and verify the malware mitigation mechanism(s) used by the third party prior to connecting the Transient Cyber Asset (per Transient Cyber Asset capability).

For Removable Media, Section 5 requires entities to employ methods to detect malicious code and mitigate the threat of detected malicious code prior to connecting to a low impact BES Cyber System.

In summary, the SDT made the following changes to address the directive:

1. Revised the definitions of Transient Cyber Asset (TCA) and Removable Media.
2. Revised Requirement R1, by adding Parts 1.2.5 and 1.2.6 to include the complementary policies for the Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation in Requirement R2 (Attachment 1 of CIP-003-7(i)).
3. Revised the requirement language (Requirement R2) in Attachment 1 of CIP-003-7 by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation.
4. Revised the associated VSLs for Requirements R1 and R2 of CIP-003-7.
5. Revised the evidential language of Attachment 2 of CIP-003-7 by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to complement the revised requirement language.

Completed Actions	Date
Standard Authorization Request approved	July 20, 2016
Draft 1 of CIP-003-7(i) posted for formal comment and initial ballot	December 9, 2016 – January 23, 2017

Anticipated Actions	Date
10-day final ballot	January, 2017
NERC Board of Trustees adoption	February, 2017
Petition filed with FERC	March, 2017

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-7(i)

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. 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 SPS or RAS where the SPS or 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-003-7(i):

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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3. 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.

4.2.3.4. 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-003-7(i).

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation; 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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1)	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1)	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the six topics required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 within 15 calendar	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the six topics required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 within 16 calendar	BES Cyber Systems, but did not address three of the six topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) 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 BES Cyber Systems 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	months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) 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 BES Cyber Systems 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	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.2)	calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2,	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing	to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but	access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR The Responsible Entity documented the determination of	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented	failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber	the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Assets and Removable Media, but 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 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2,		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 5.3. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. 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 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.	

Version	Date	Action	Change Tracking
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 devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7(i)	TBD	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.

Attachment 1

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

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

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

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

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The

focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

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

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

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

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security

Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Rationale for Section 5 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

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

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

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

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, the use of one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;

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

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

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

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

Attachment 2

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

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

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

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

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

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

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

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

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

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability

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.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents

- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media
- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a

combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such

communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located

at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

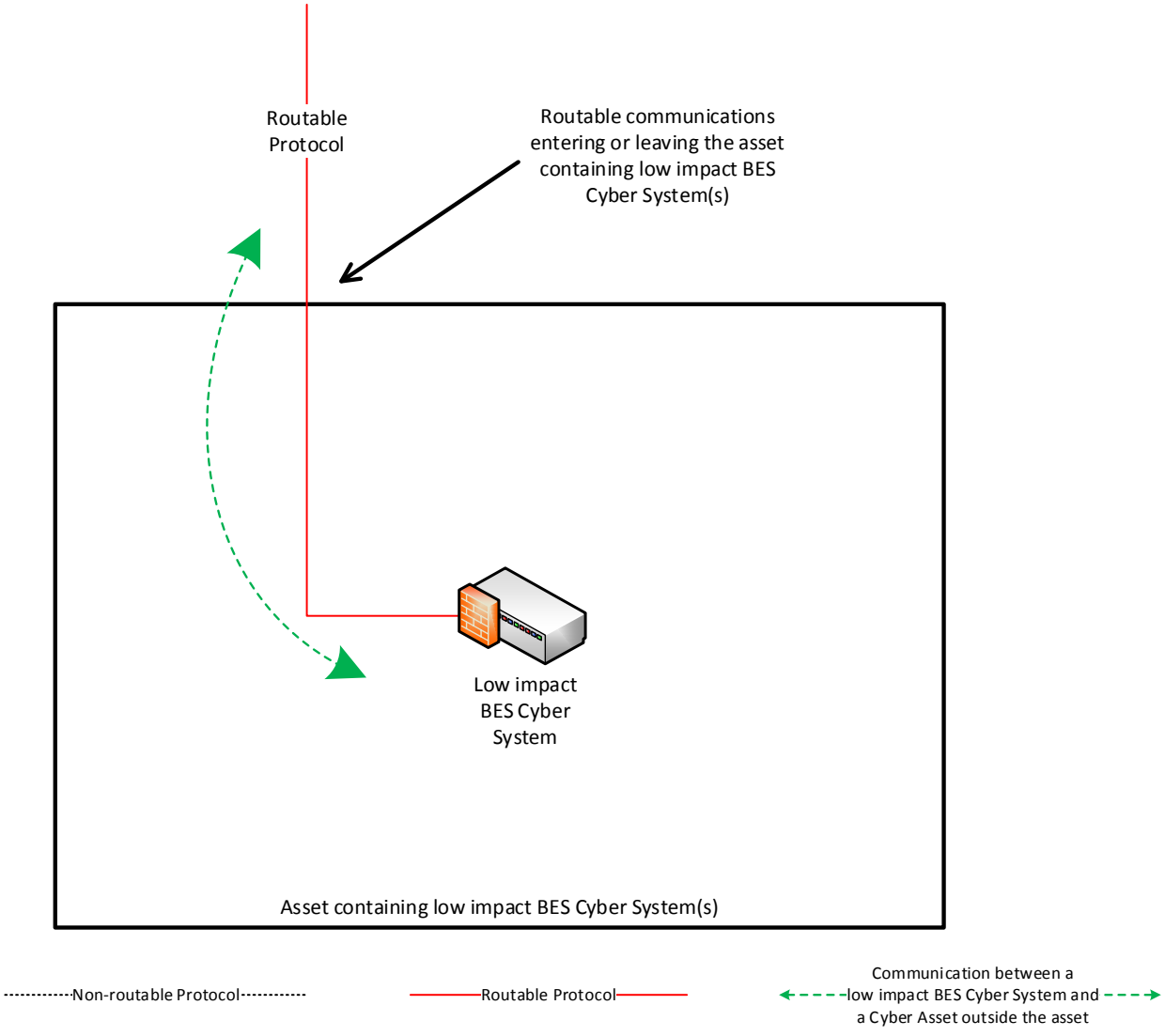
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

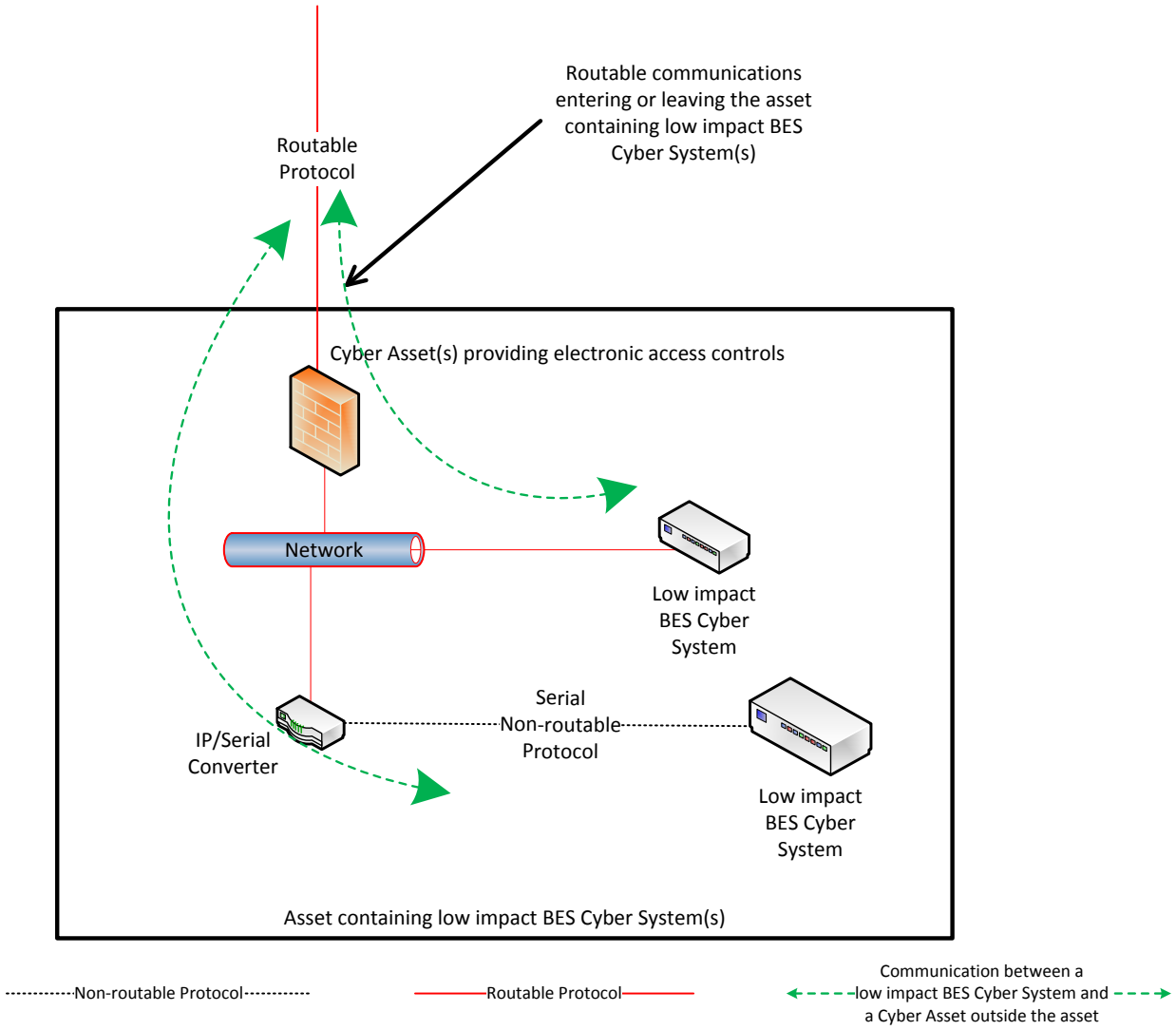
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

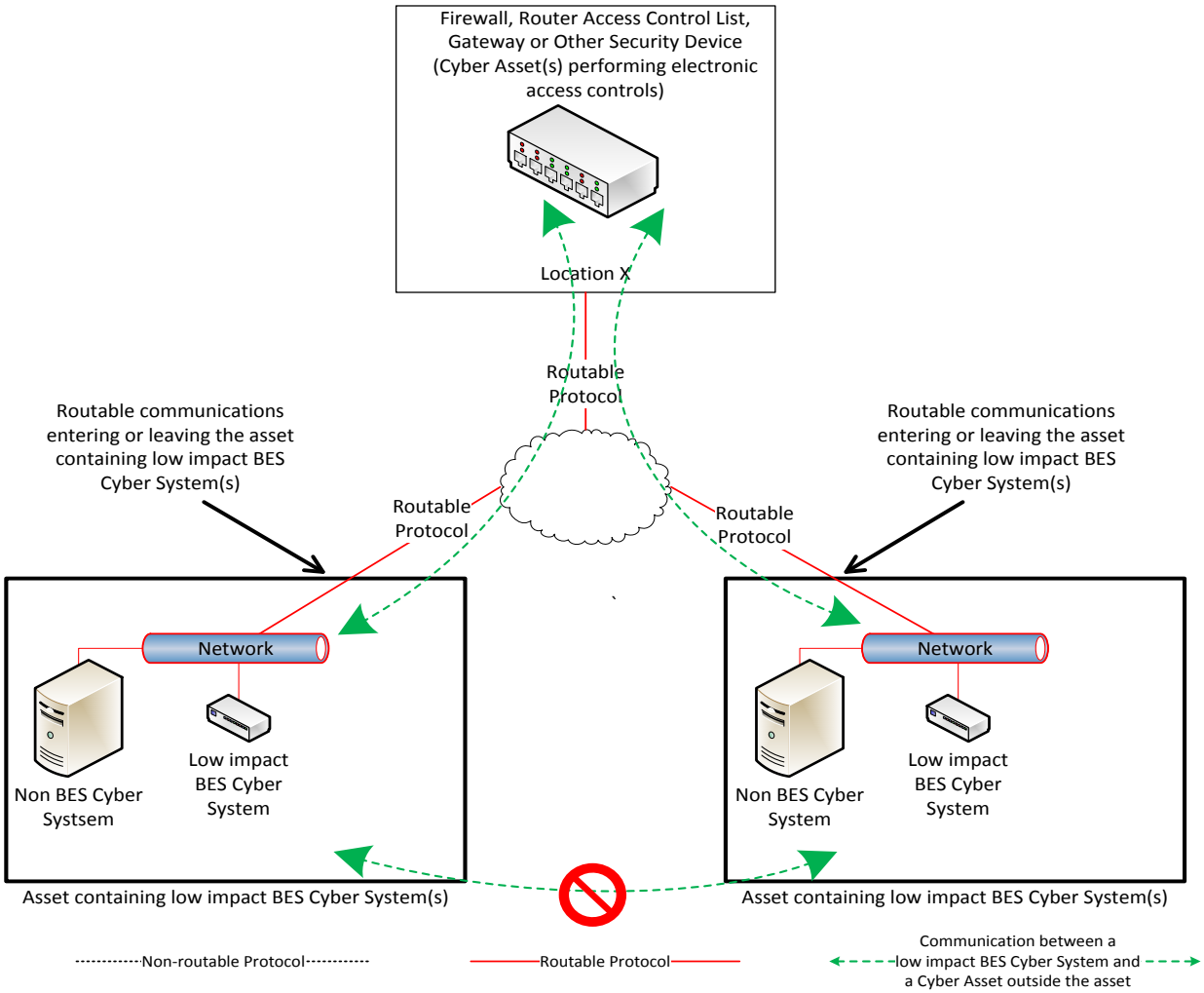
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

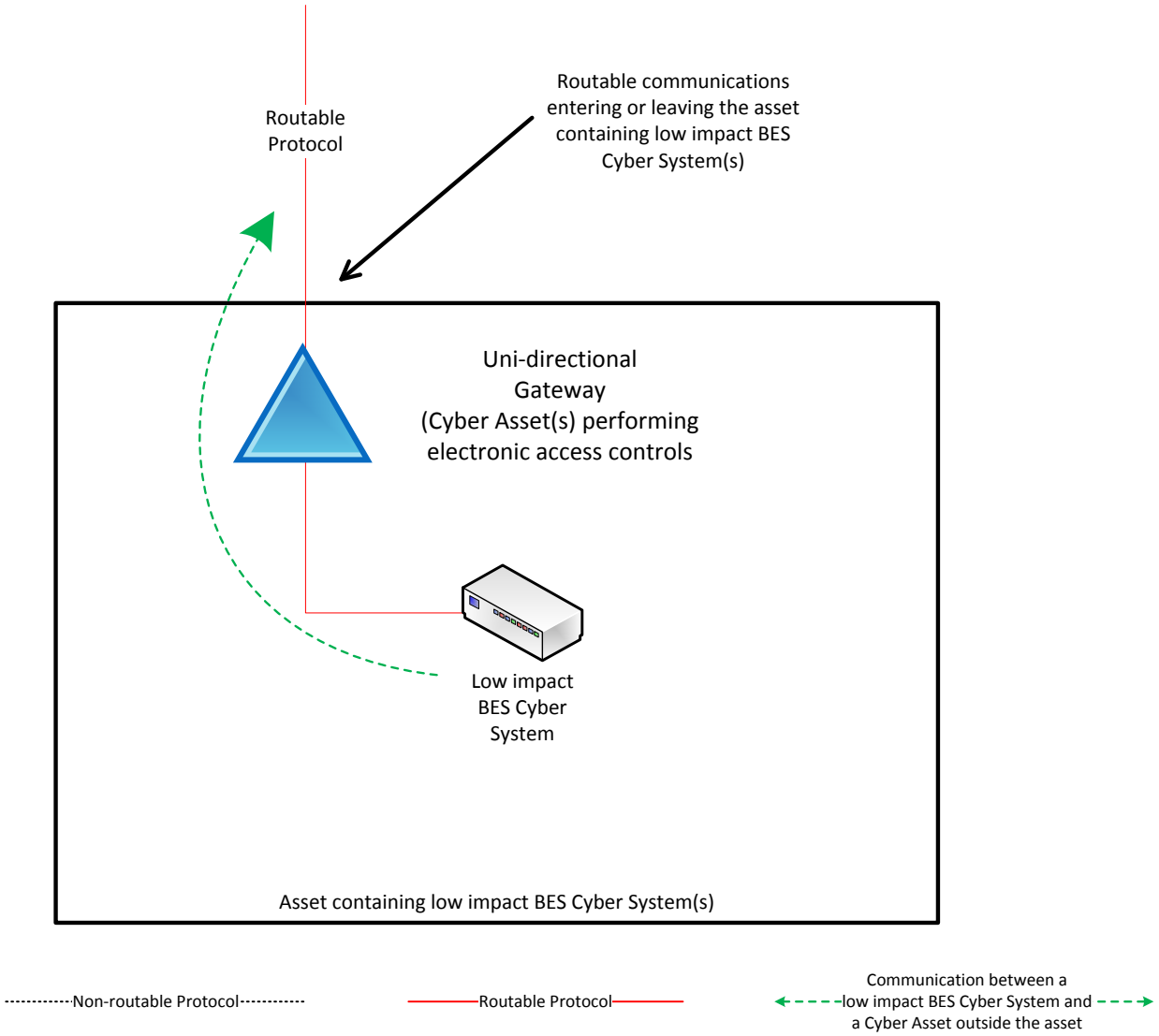
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

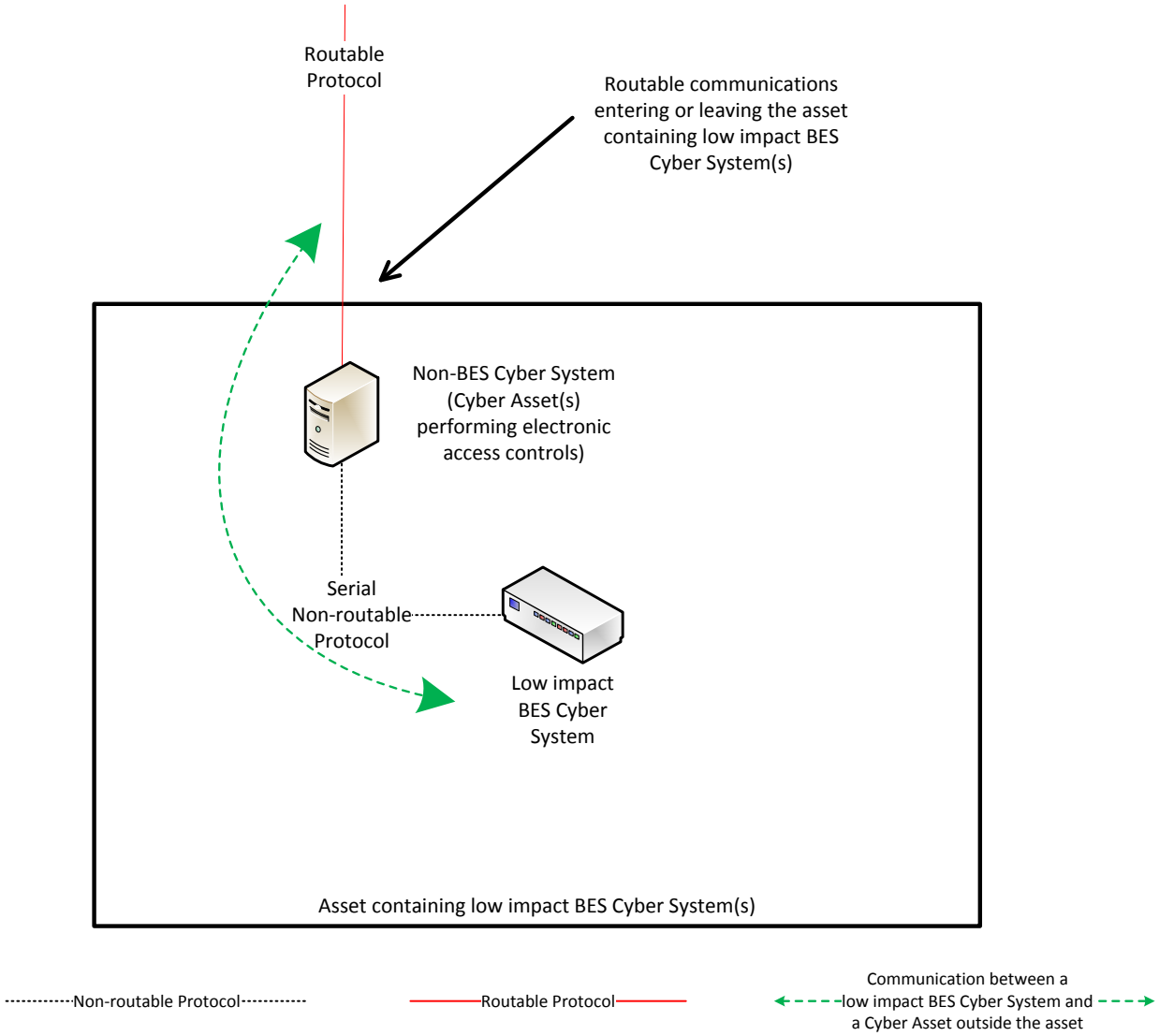
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

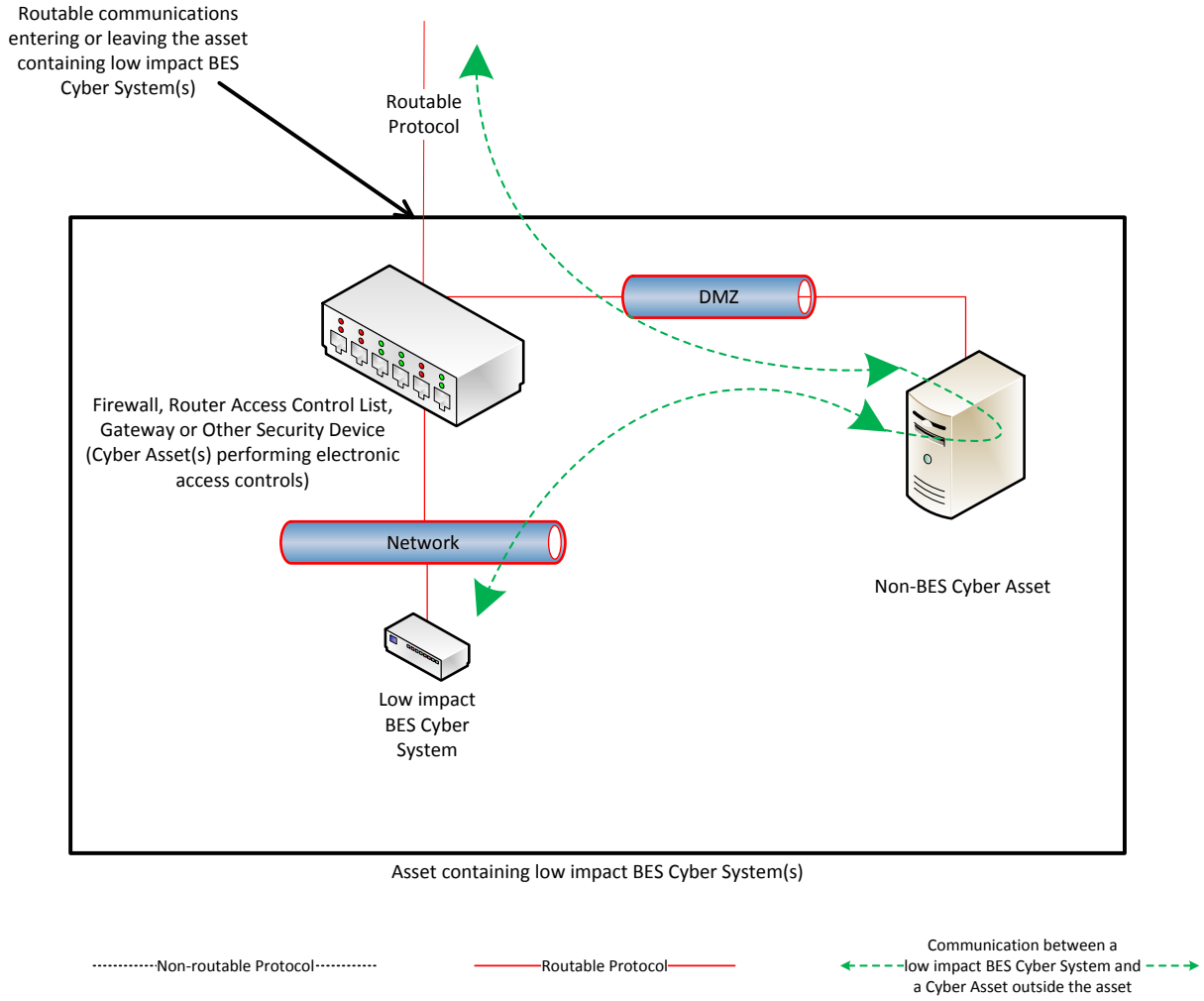
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

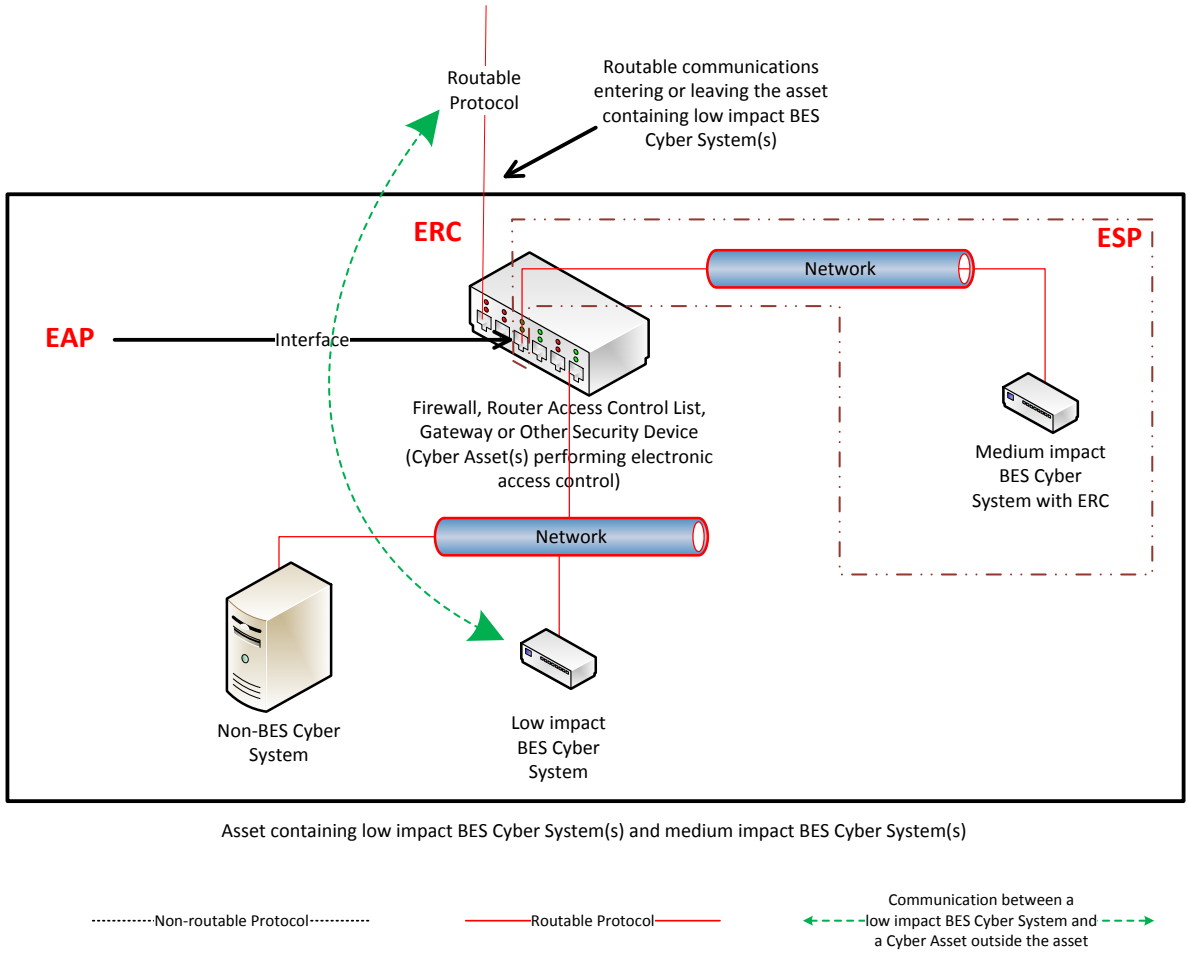
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.

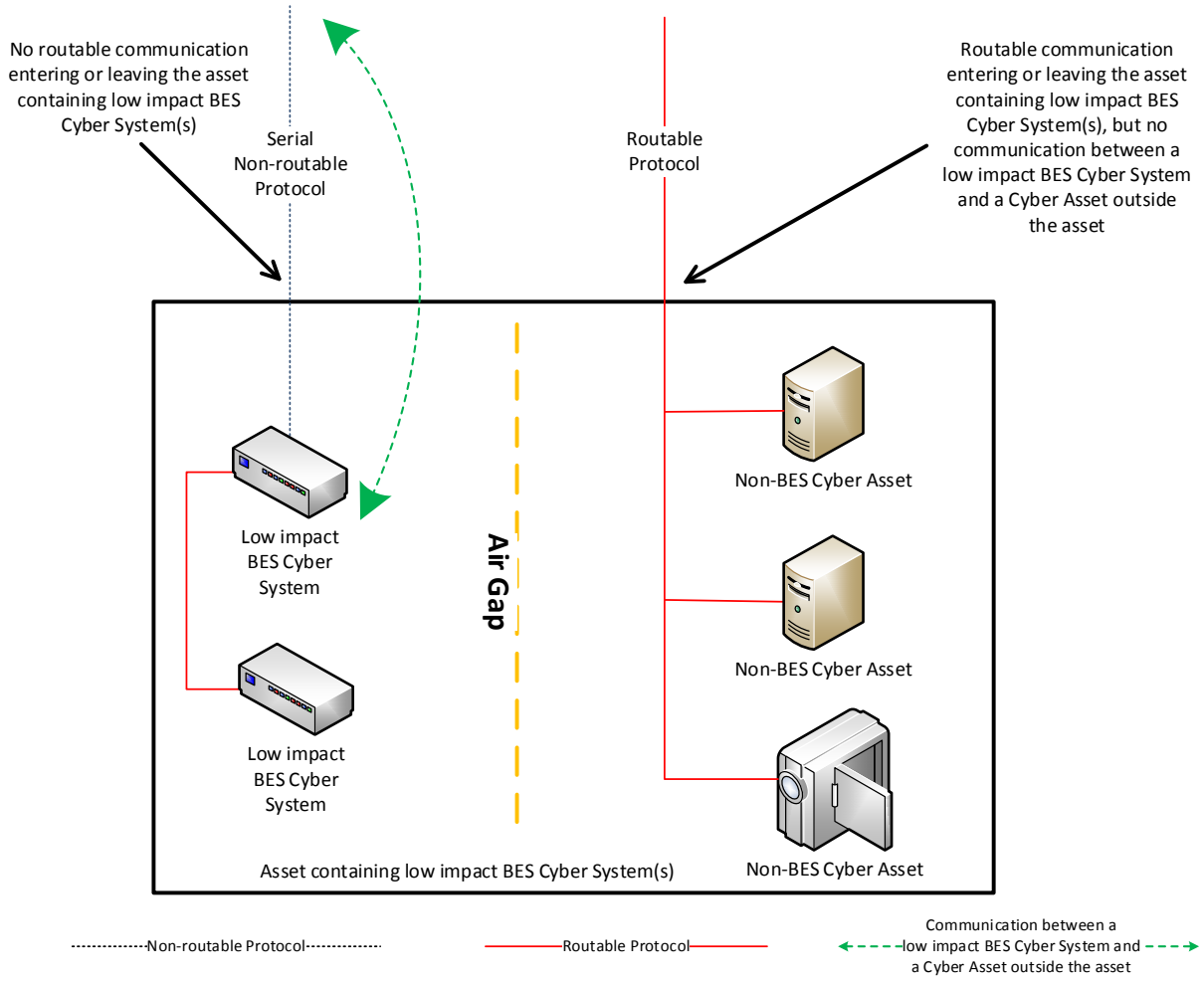


Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

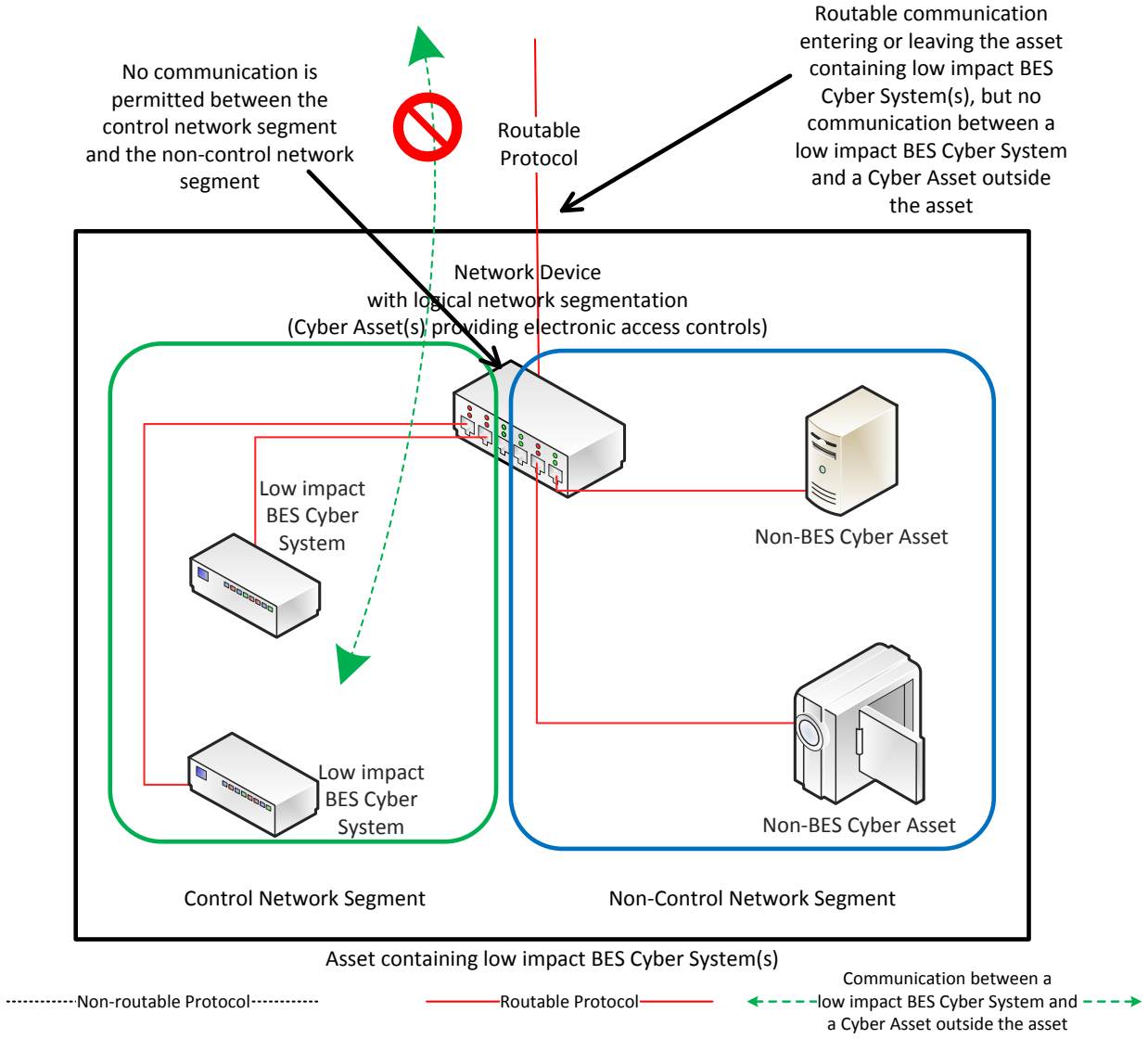
1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

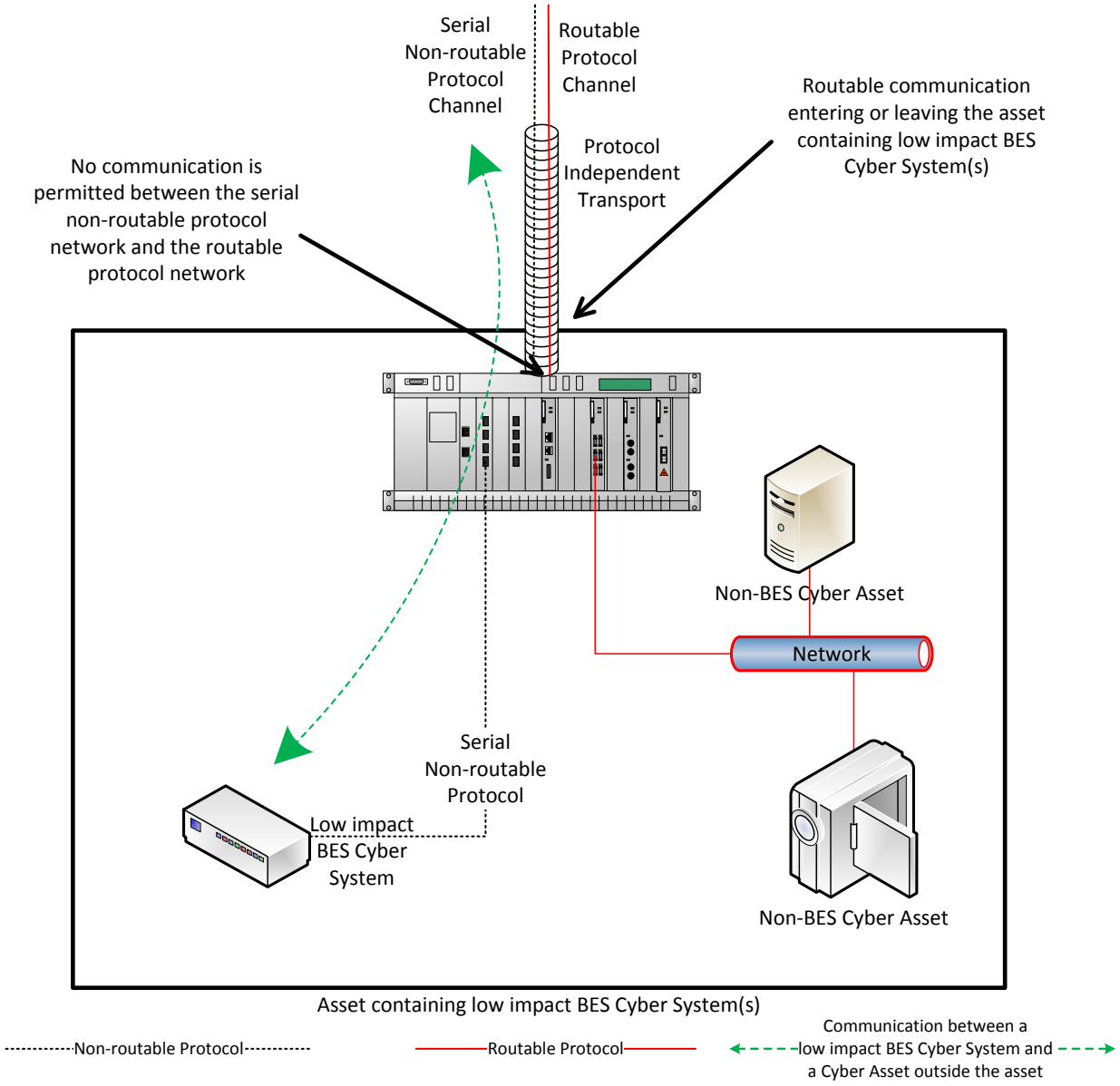
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Malicious Code Risk Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that

can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives

the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for “clear lines of authority and ownership for security matters.” With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

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.

Description of Current Draft

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions to be incorporated into the Glossary of Terms Used in NERC Reliability Standards. In addition to approving the seven CIP Reliability Standards, the Commission, directed NERC to, among other things,: (1) "…develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems…", and (2) modify the definition of LERC.

In response to these directives, NERC first modified Reliability Standard CIP-003-6 to address the LERC directive~~,~~ which has a regulatory deadline of March 31, 2017 for filing with the Commission. The revisions associated with the LERC directive were developed and posted for comment and ballot in July 2016 in draft Reliability Standard CIP-003-7. The revisions were not approved by stakeholders and based on the feedback received, the drafting team revised its approach and posted the revisions for an additional comment period and ballot. CIP-003-7 passed the additional ballot that ended on December 5, 2016.

For the transient device directive, NERC initially posted draft revisions for an informal comment period from November 1-18, 2016. This draft of Reliability Standard CIP-003-7(i) incorporates the proposed TCA language, as modified based on stakeholder comment, with the recently passed LERC revisions. The intent of this approach is to allow entities time to efficiently plan and implement the required modifications for low impact BES Cyber Systems. The Standard Drafting Team (SDT) approach to address the transient device directive is summarized below.

The SDT revised Attachment 1 of CIP-003-7 to include requirements that mitigate the risk to the BES of malware propagation from transient devices to low impact BES Cyber Systems. Attachment 1 contains and outlines the required sections of a Responsible Entity's cyber security plan(s) for its low impact BES Cyber Systems per Requirement R2. Previously, cyber security plan(s) were required to address four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. In keeping with the stakeholder approved approach to incorporate into one standard all the requirements applicable to assets containing low impact BES Cyber Systems, the SDT expanded CIP-003-7 Attachment 1 to include a fifth area: "Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation." Requiring the Responsible Entity to develop and implement these plans will provide higher assurance against the propagation of malware from transient devices.

In addition, the SDT determined it was necessary to revise the definitions of a Transient Cyber Asset (TCA) and Removable Media to ensure applicability of security controls and provide additional clarity. As well, the revised definitions accommodate use of the terms for all impact

levels: high, medium, and low. This is important for those entities that may opt to deploy one program to manage TCAs and Removable Media across multiple impact level assets.

The proposed revised definition of a Transient Cyber Asset (TCA) is:

A Cyber Asset that is:

1. *capable of transmitting or transferring executable code,*
2. *not included in a BES Cyber System,*
3. *not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and*
4. *directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:*
    - *BES Cyber Asset,*
    - *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
    - *PCA associated with high or medium impact BES Cyber Systems.*

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

The proposed revised definition of Removable Media is:

Storage media that:

1. *are not Cyber Assets,*
2. *are capable of transferring executable code,*
3. *can be used to store, copy, move, or access data, and*
4. *are directly connected for 30 consecutive calendar days or less to a:*
    - *BES Cyber Asset,*
    - *network within an Electronic Service Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
    - *Protected Cyber Asset associated with high or medium impact BES Cyber Systems.*

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

As proposed, Section 5 of Attachment 1 of CIP-003-7(i) mandates that entities have malware protection on TCAs (both entity and vendor-managed) and for Removable Media. The SDT proposes that it is necessary to distinguish between the specific protections for: (i) TCAs managed by the Responsible Entity, (ii) TCAs managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media.

For TCAs managed by the Responsible Entity, Section 5 requires the Responsible Entity to use one or a combination of the following to mitigate the introduction of malicious code: antivirus software, application whitelisting, or some other method. The SDT recognizes that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices (i.e., manage in an ongoing manner) while others have a checklist for transient devices prior to connecting them to a BES Cyber System (i.e., manage in an on-demand manner). The SDT acknowledges that both methods are effective and Section 5 permits either form of management. Because of the higher frequency in which these entity-managed devices are used, the controls required for these devices are more specific.

For Transient Cyber Assets managed by a party other than the Responsible Entity, Section 5 requires the Responsible Entity to review and verify the malware mitigation mechanism(s) used by the third party prior to connecting the Transient Cyber Asset (per Transient Cyber Asset capability).

For Removable Media, Section 5 requires entities to employ methods to detect malicious code and mitigate the threat of detected malicious code prior to connecting to a low impact BES Cyber System.

In summary, the SDT made the following changes to address the directive:

1. Revised the definitions of Transient Cyber Asset (TCA) and Removable Media.
2. Revised Requirement R1, by adding Parts 1.2.5 and 1.2.6 to include the complementary policies for the Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation in Requirement R2 (Attachment 1 of CIP-003-7(i)).
3. Revised the requirement language (Requirement R2) in Attachment 1 of CIP-003-7 by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation.
4. Revised the associated VSLs for Requirements R1 and R2 of CIP-003-7.
5. Revised the evidential language of Attachment 2 of CIP-003-7 by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to complement the revised requirement language.

Completed Actions	Date
Standard Authorization Request approved	July 20, 2016
Draft 1 of CIP-003-7(i) posted for formal comment and initial ballot	December 9, 2016 – January 23, 2017

Anticipated Actions	Date
10-day final ballot	~~February~~January, 2017
NERC Board of Trustees adoption	February, 2017
Petition filed with FERC	March, 2017

A. Introduction

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

2. **Number:** CIP-003-7(i)

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

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 Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or 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. Interchange Coordinator or Interchange Authority

   4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. 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 SPS or RAS where the SPS or 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-003-7(i):

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 discrete Electronic Security Perimeters (ESPs).

4.2.3.3. 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.

4.2.3.4. 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-003-7(i).

6. Background:

Standard CIP-003 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 organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

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 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.

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 Reliability 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, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. 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 BES. 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.

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 BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media ~~M~~malicious ~~C~~code ~~R~~risk ~~M~~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 BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) 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 CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1)	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1.1)	calendar months of the previous review. (R1.1) 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 BES Cyber Systems as required by 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. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (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 impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the six topics required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 within 15 calendar	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the six topics required by R1. (R1.2) 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 BES Cyber Systems as required by Requirement R1 within 16 calendar	BES Cyber Systems, but did not address three of the six topics required by R1. (R1.2) 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 BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) 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 BES Cyber Systems 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	months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) 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 BES Cyber Systems 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	assets identified in CIP-002 containing low impact BES Cyber Systems 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. (R1.2)	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 BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.2)	calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2,	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing	to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but	access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but 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. (R2) OR The Responsible Entity documented the determination of	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented	failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			its plan(s) for Transient Cyber Assets ~~and Removable Media~~, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the 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 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but 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. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber	the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Assets and Removable Media, but 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 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2,		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 5.3. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but 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. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-7(i))			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Formatted: Width: 8.5", Height: 11"

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.	

Version	Date	Action	Change Tracking
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 devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7(i)	TBD	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.

Attachment 1

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

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

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

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

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The

focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

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

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

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

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

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

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security

Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Rationale for Section 5 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

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

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

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

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, the use of one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;

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

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

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

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

Attachment 2

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

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

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

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

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

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

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

Formatted: No underline

Formatted: No underline

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

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

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability

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.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-7, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-7, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-7, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity ~~should~~ may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents

- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media
- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a

combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such

communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located

at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

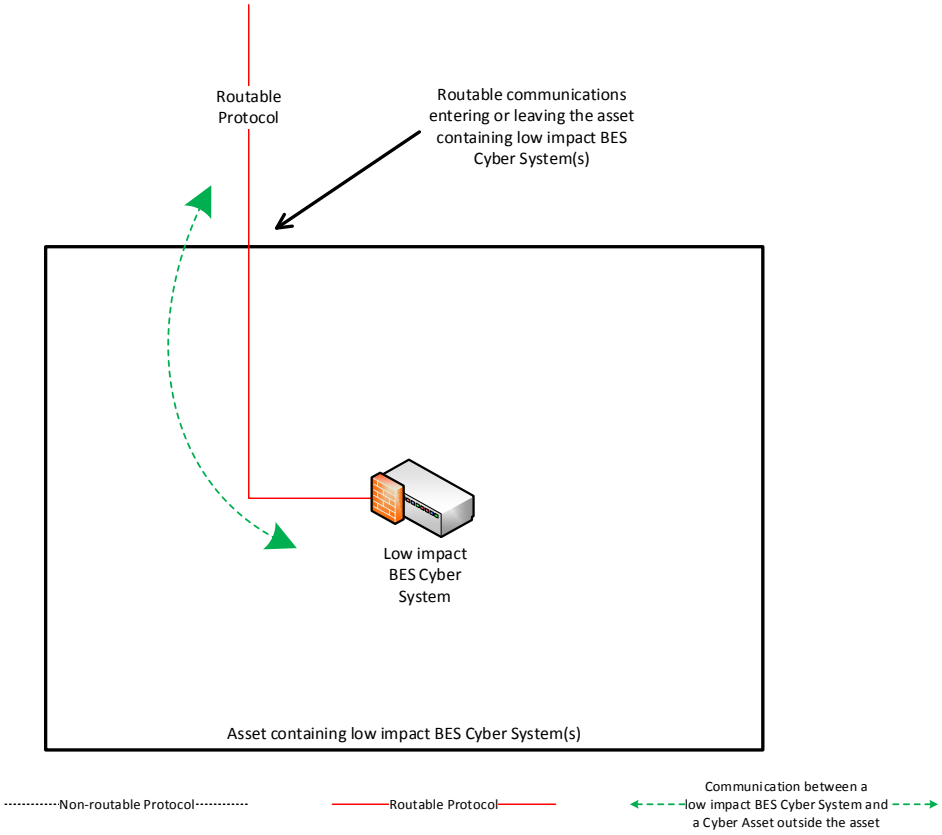
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

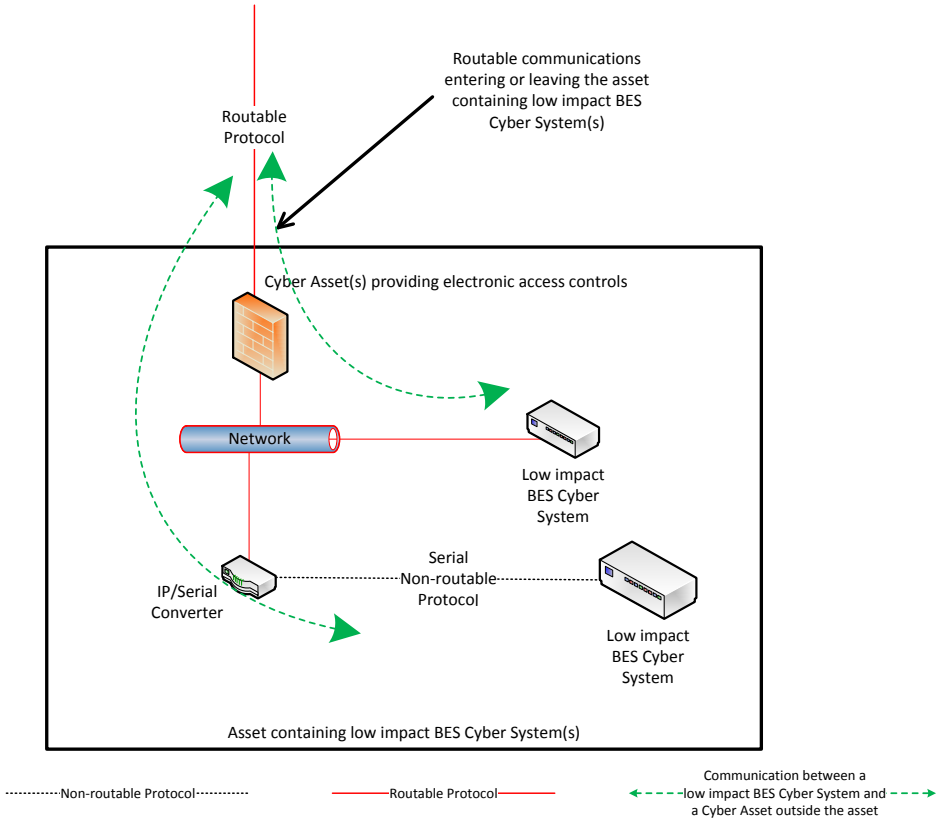
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

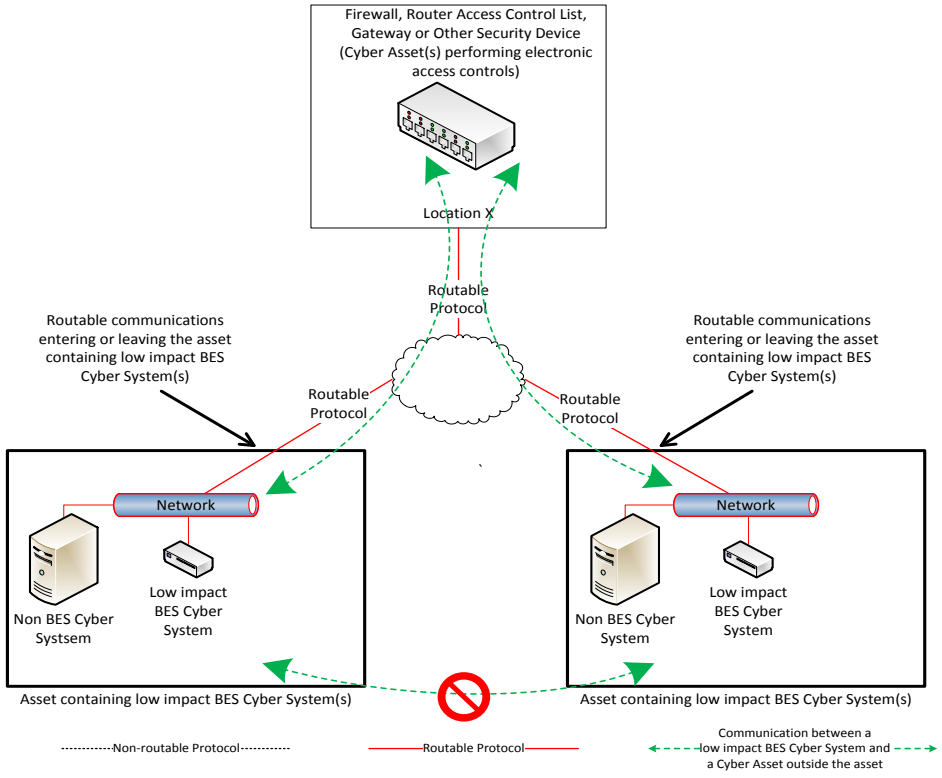
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

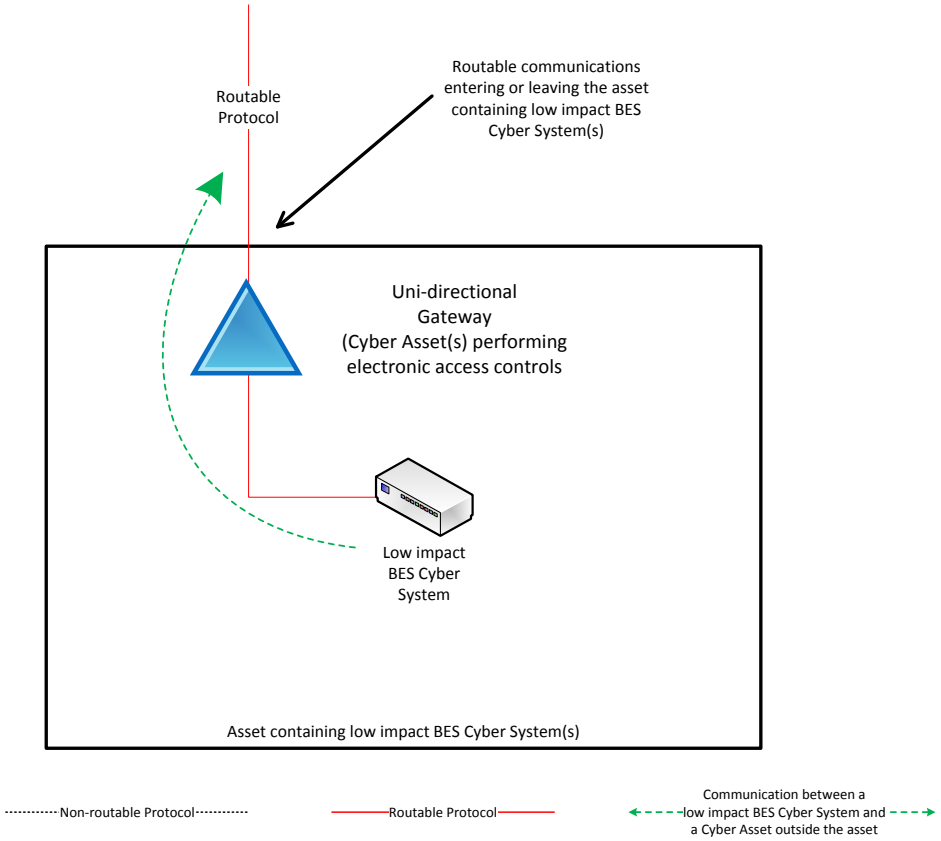
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

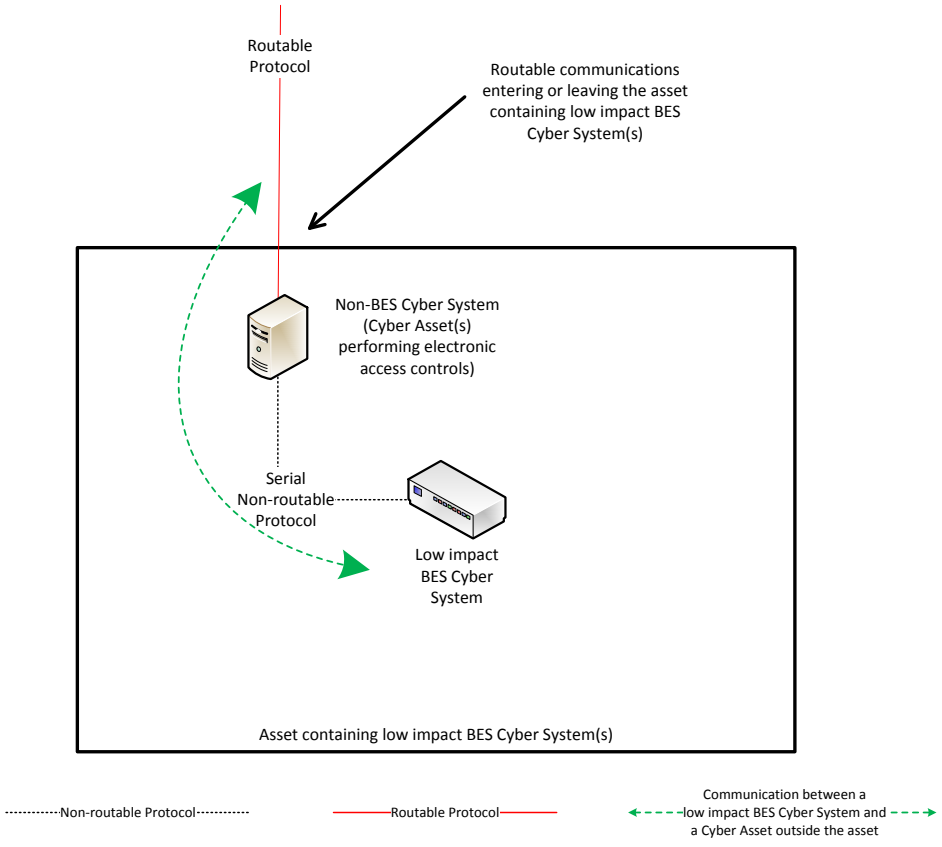
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

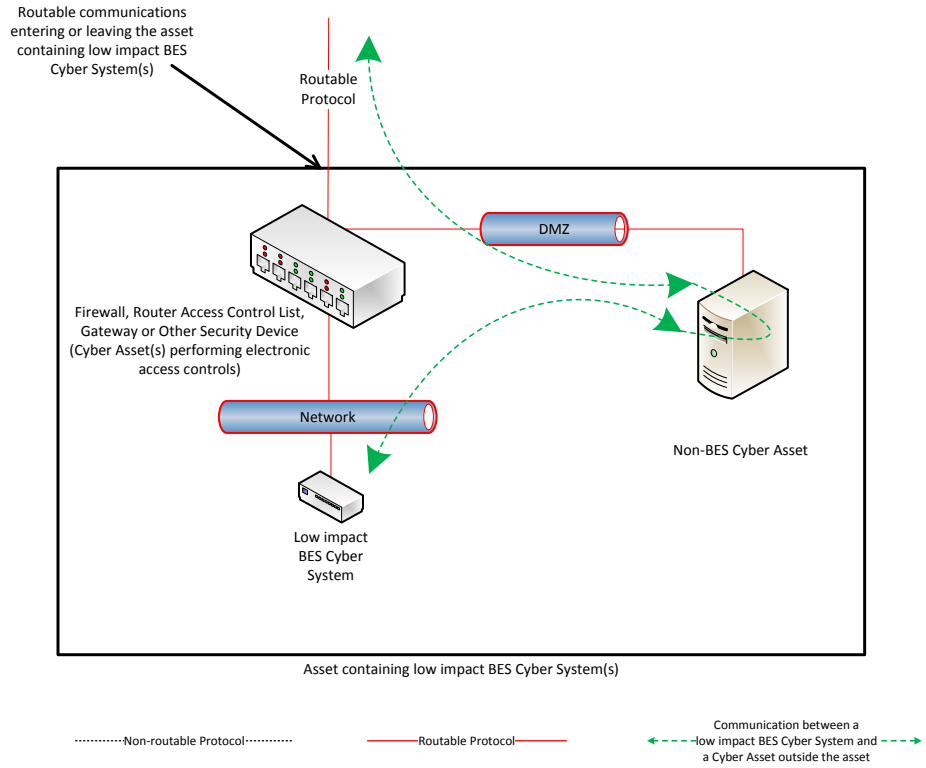
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

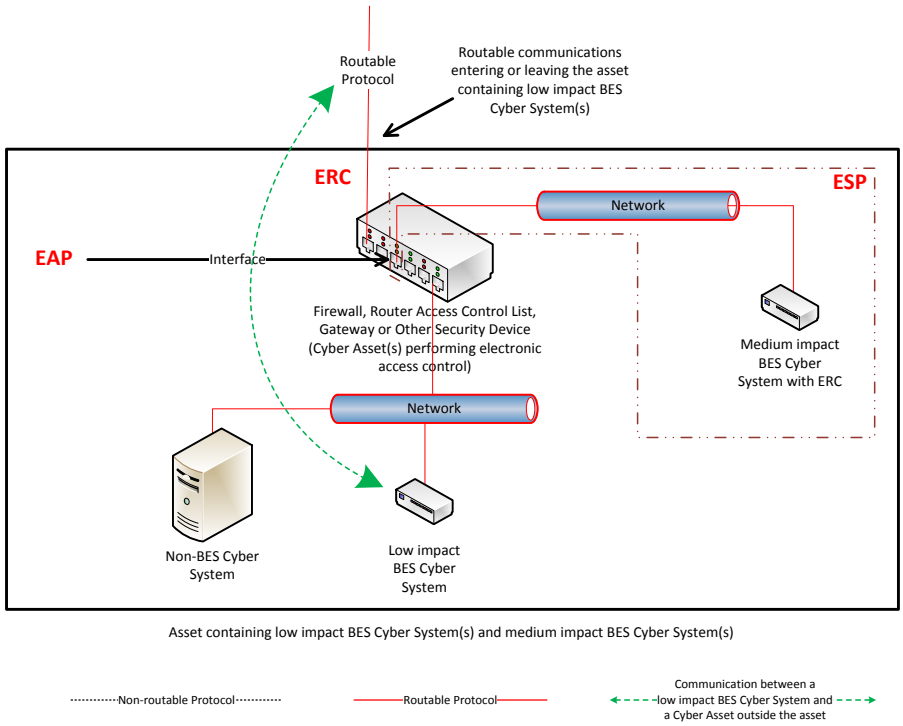
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.

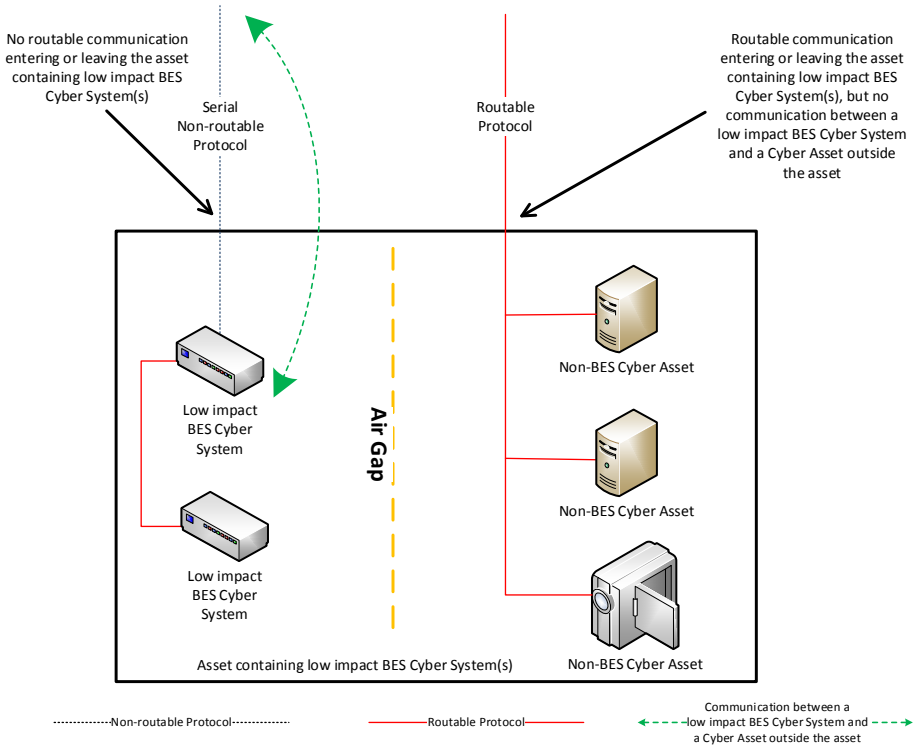


Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

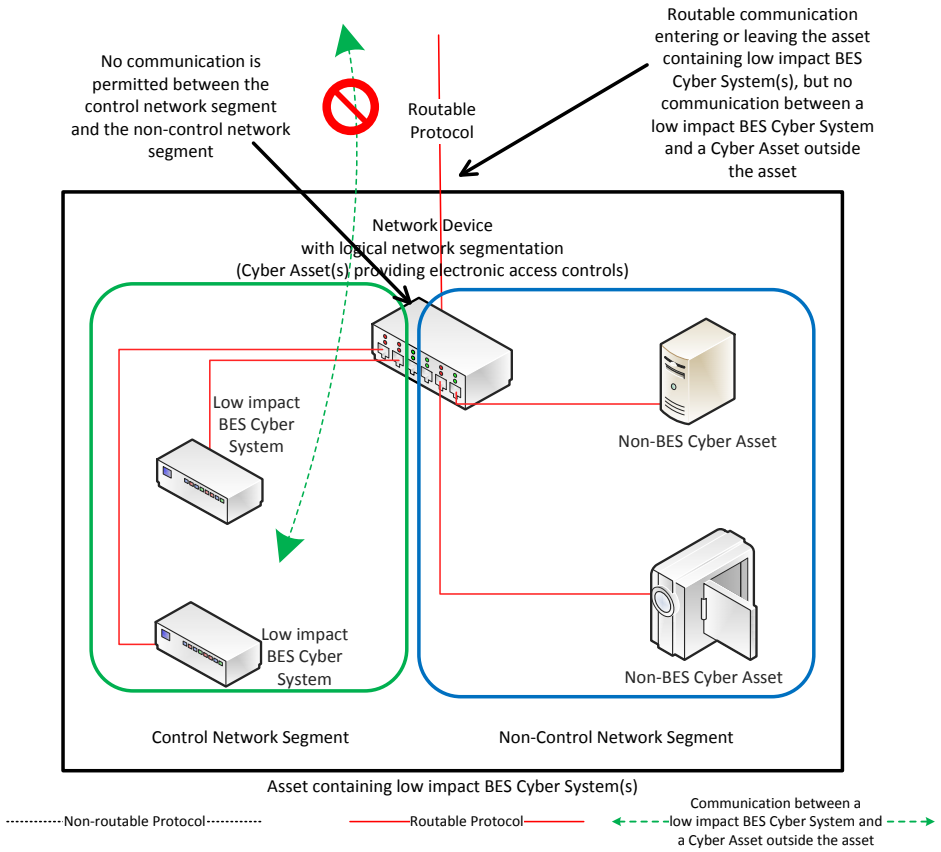
1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

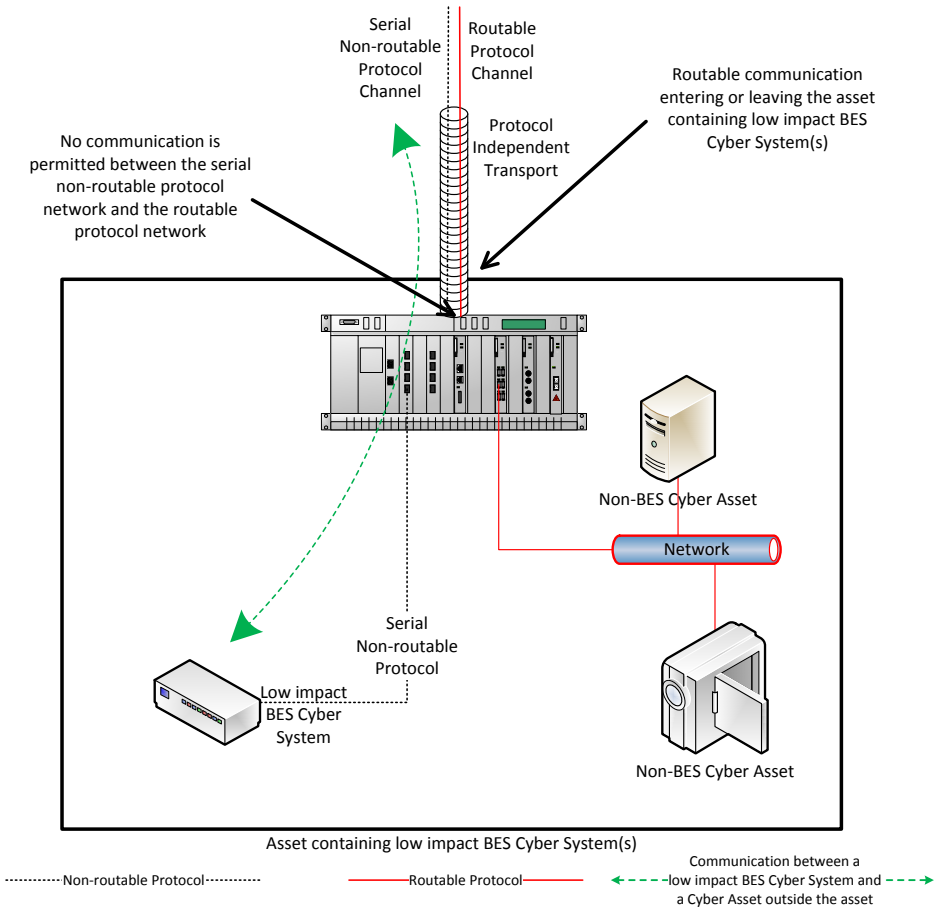
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore ~~Responsible Entitieis need~~ Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices~~, including~~ from a specially-designed device~~s~~ for maintaining equipment in support of the BES ~~or~~to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

~~Vulnerability~~Malicious Code Risk Mitigation

The terms "mitigate", "mitigating", and "mitigation" are used in ~~the sections~~Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. ~~Mitigation in this context does not necessarily require that each vulnerability be individually addressed or remediated, as many vulnerabilities may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected.~~ Mitigation is intended to mean that entities ~~take steps to~~ reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their ~~process(es~~plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset. ~~When addressing malicious code protection, Section 5.1 obligates the Responsible Entities to implement methods to mitigate the introduction of malicious code on Transient Cyber Assets managed by the Responsible Entity.~~

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s),

the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

~~Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

The following is ~~some~~ additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- ~~If a Responsible Entity chooses touse~~ When using methods ~~that mitigate the introduction of malicious code~~ other than those listed, ~~it should documentat~~entities need to document how the other method(s) meet the ~~mitigation~~objective of mitigating the risk of the introduction of malicious code ~~objective~~.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent ~~it~~the malicious code from being introduced into the BES Cyber ~~Asset or~~ System. ~~Alternatively, if malicious code is discovered, a~~An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security

practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. ~~is t~~The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is ~~also~~ to not ~~to~~ require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party~~'s~~ and entity~~'s~~ actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities ~~should~~may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method~~asure~~

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

~~helps~~ intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. ~~However, t~~The SDT does not intend to obligate ~~for~~ a Responsible Entity to conduct a review for every single connection of ~~that~~ Removable Media, but rather to implement ~~their~~ its plan~~rocess~~(~~e~~s) in a manner that protects all BES Cyber Systems where ~~the~~ Removable Media may be used. The intent is ~~also~~ to not ~~to~~ require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-7, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-7, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as

long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives

the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-003-7(i) - Cyber Security – Security Management Controls

Requested Approvals

- Reliability Standard CIP-003-7(i) - Cyber Security – Security Management Controls
- Definition of Transient Cyber Asset (TCA)
- Definition of Removable Media

Requested Retirements

- Reliability Standard CIP-003-6 - Cyber Security – Security Management Control
- Definition Low Impact BES Cyber System Electronic Access Point (LEAP)
- Definition of Low Impact External Routable Connectivity (LERC)
- Definition of Transient Cyber Asset (TCA)
- Definition of Removable Media

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions to be incorporated into the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary). In addition to approving the seven CIP Reliability Standards, the Commission, among other things, directed NERC to: (1) "develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems"; and (2) modify the definition of LERC in the NERC Glossary.

With respect to the transient devices directive, the Commission stated:

> 32. After consideration of the comments received on this issue, we conclude that the adoption of controls for transient devices used at Low Impact BES Cyber Systems, including Low Impact Control Centers, will provide an important enhancement to the security posture of the bulk electric system by reinforcing the defense-in-depth nature of the CIP Reliability Standards at all impact levels. Accordingly, we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.

For the LERC directive, the Commission stated:

> 73. Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

To address these directives, NERC modified Reliability Standard CIP-003. In responding to the transient devices directive, NERC modified the definitions of TCA and Removable Media. The revised definitions ensure the applicability of security controls, provide clarity, and accommodate the use of the terms for all impact levels: high, medium and low. The revised definitions will allow entities to deploy one program to manage TCAs and Removable Media across multiple impact levels.

Further, as an alternative to modifying the LERC definition, the standard drafting team retired the terms "LERC" and "LEAP", incorporating those concepts within the requirement language.

General Considerations

This Implementation Plan does not modify the effective date for CIP-003-6 in the Implementation Plan associated with CIP-003-6 nor any of the phased-in compliance dates included therein except that the compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7(i), provided in this Implementation Plan.

Further, this Implementation Plan clarifies that under Requirement R2 of CIP-003-7(i), the Responsible Entity shall not be required to include in its cyber security plan(s) any elements related to Sections 2, 3, and 5 of Attachment 1 until the effective date of CIP-003-7(i). Upon the effective date of CIP-003-7(i), the Responsible Entity's cyber security plan(s) must include the elements required by Sections 2, 3, and 5 of Attachment 1 and the Responsible Entity must implement the controls included in its plan to meet the objectives of Sections 2, 3, and 5.

Effective Dates

The effective dates for the proposed Reliability Standard and NERC Glossary terms are provided below.

Reliability Standard CIP-003-7(i)

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7(i) shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-7(i) shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

NERC Glossary Definitions of Transient Cyber Asset and Removable Media

Where approval by an applicable governmental authority is required, the definitions of Transient Cyber Asset and Removable Media shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the definitions, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the definitions of Transient Cyber Asset and Removable Media shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the date that the definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Planned or Unplanned Changes

Planned or Unplanned Changes Resulting in a Higher Categorization – This Implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-5 titled Planned or Unplanned Changes Resulting in a Higher Categorization.[1]

Unplanned Changes Resulting in Low Impact Categorization – This Implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-6 titled Unplanned Changes Resulting in Low Impact Categorization. That section provides:

> For unplanned changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

Retirement Date

Reliability Standard CIP-003-6

Reliability Standard CIP-003-6 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-7(i) in the particular jurisdiction in which the revised standard is becoming effective.

Current NERC Glossary of Terms Definition(s) of LERC, LEAP, TCA and Removable Media

The current definitions of LERC and LEAP shall be retired from the NERC Glossary immediately prior to the effective date of Reliability Standard CIP-003-7(i) in the particular jurisdiction in which the revised standard is becoming effective.

The current definitions of Transient Cyber Asset and Removable Media shall be retired from the NERC Glossary immediately prior to the effective date of the revised definitions for those terms in the particular jurisdiction in which the revised definitions are becoming effective.

[1] Due to the length of that section, it is not reproduced herein.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-003-7(i) - Cyber Security – Security Management Controls

Requested Approvals

- Reliability Standard CIP-003-7(i) - Cyber Security – Security Management Controls
- Definition of Transient Cyber Asset (TCA)
- Definition of Removable Media

Requested Retirements

- Reliability Standard CIP-003-6 - Cyber Security – Security Management Control
- Definition Low Impact BES Cyber System Electronic Access Point (LEAP)
- Definition of Low Impact External Routable Connectivity (LERC)
- Definition of Transient Cyber Asset (TCA)
- Definition of Removable Media

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions to be incorporated into the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary). In addition to approving the seven CIP Reliability Standards, the Commission, among other things, directed NERC to: (1) "develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems"; and (2) modify the definition of LERC in the NERC Glossary.

With respect to the transient devices directive, the Commission stated:

> 32. After consideration of the comments received on this issue, we conclude that the adoption of controls for transient devices used at Low Impact BES Cyber Systems, including Low Impact Control Centers, will provide an important enhancement to the security posture of the bulk electric system by reinforcing the defense-in-depth nature of the CIP Reliability Standards at all impact levels. Accordingly, we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.

For the LERC directive, the Commission stated:

> 73. Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

To address these directives, NERC modified Reliability Standard CIP-003. In responding to the transient devices directive, NERC modified the definitions of TCA and Removable Media. The revised definitions ensure the applicability of security controls, provide clarity, and accommodate the use of the terms for all impact levels: high, medium and low. The revised definitions will allow entities to deploy one program to manage TCAs and Removable Media across multiple impact levels.

Further, as an alternative to modifying the LERC definition, the standard drafting team retired the terms "LERC" and "LEAP", incorporating those concepts within the requirement language.

General Considerations

This Implementation Plan does not modify the effective date for CIP-003-6 in the Implementation Plan associated with CIP-003-6 nor any of the phased-in compliance dates included therein except that the compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7(i), provided in this Implementation Plan.

Further, this Implementation Plan clarifies that under Requirement R2 of CIP-003-7(i), the Responsible Entity shall not be required to include in its cyber security plan(s) any elements related to Sections 2, 3, and 5 of Attachment 1 until the effective date of CIP-003-7(i). Upon the effective date of CIP-003-7(i), the Responsible Entity's cyber security plan(s) must include the elements required by Sections 2, 3, and 5 of Attachment 1 and the Responsible Entity must implement the controls included in its plan to meet the objectives of Sections 2, 3, and 5.

Effective Dates

The effective dates for the proposed Reliability Standard and NERC Glossary terms are provided below.

Reliability Standard CIP-003-7(i)

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7(i) shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-7(i) shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

NERC Glossary Definitions of Transient Cyber Asset and Removable Media

Where approval by an applicable governmental authority is required, the definitions of Transient Cyber Asset and Removable Media shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the definitions, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the definitions of Transient Cyber Asset and Removable Media shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the date that the definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Planned or Unplanned Changes

Planned or Unplanned Changes Resulting in a Higher Categorization – This Implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-5 titled Planned or Unplanned Changes Resulting in a Higher Categorization.[1]

Unplanned Changes Resulting in Low Impact Categorization – This Implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-6 titled Unplanned Changes Resulting in Low Impact Categorization. That section provides:

> For unplanned changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

Retirement Date

Reliability Standard CIP-003-6

Reliability Standard CIP-003-6 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-7(i) in the particular jurisdiction in which the revised standard is becoming effective.

Current NERC Glossary of Terms Definition(s) of LERC, LEAP, TCA and Removable Media

The current definitions of LERC and LEAP shall be retired from the NERC Glossary immediately prior to the effective date of Reliability Standard CIP-003-7(i) in the particular jurisdiction in which the revised standard is becoming effective.

The current definitions of Transient Cyber Asset and Removable Media shall be retired from the NERC Glossary immediately prior to the effective date of the revised definitions for those terms in the particular jurisdiction in which the revised definitions are becoming effective.

[1] Due to the length of that section, it is not reproduced herein.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed Definitions of: "Transient Cyber Asset" (TCA) and "Removable Media"

Term: "Transient Cyber Asset" (TCA)

Revised Definition:

A Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Redline Definition:

A Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Currently Approved Definition of "Transient Cyber Asset" (TCA):

A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Term: "Removable Media"

Revised Definition:

Storage media that:

1. are not Cyber Assets,
2. are capable of transferring executable code,
3. can be used to store, copy, move, or access data, and
4. are directly connected for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Redline Definition:

Storage media that:

1. are not Cyber Assets,
2. are capable of transferring executable code,
3. can be used to store, copy, move, or access data, and
4. are directly connected for 30 consecutive calendar days or less to a:
   - BES Cyber Asset, ~~a~~
   - network within an Electronic Security Perimeter (ESP)~~,~~ containing high or medium impact BES Cyber Systems, or ~~a~~
   - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Currently Approved Definition of "Removable Media":

Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed Definitions of: "Transient Cyber Asset" (TCA) and "Removable Media"

Term: "Transient Cyber Asset" (TCA)

Revised Definition:

A Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Redline Definition:

A Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Currently Approved Definition of "Transient Cyber Asset" (TCA):

A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Term: "Removable Media"

Revised Definition:

Storage media that:

1. are not Cyber Assets,
2. are capable of transferring executable code,
3. can be used to store, copy, move, or access data, and
4. are directly connected for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Redline Definition:

Storage media that:

1. are not Cyber Assets,
2. are capable of transferring executable code,
3. can be used to store, copy, move, or access data, and
4. are directly connected for 30 consecutive calendar days or less to a:
   - BES Cyber Asset, ~~a~~
   - network within an Electronic Security Perimeter (ESP)~~,~~ containing high or medium impact BES Cyber Systems, or ~~a~~
   - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Currently Approved Definition of "~~Transient Cyber Asset~~Removable Media"~~ (TCA)~~:

Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards
CIP-003-7(i)

Final Ballots Open through February 8, 2017

Now Available

10-day final ballots for the following are open through **8 p.m. Eastern, Wednesday, February 8, 2017**:

1. **CIP-003-7(i) - Cyber Security – Security Management Controls**
2. **CIP-003-7(i) Implementation Plan**
3. **Transient Cyber Asset (TCA) - Proposed revised definition**
4. **Removable Media - Proposed revised definition**

Balloting

In the final ballot, votes are counted by exception. Votes from the previous ballot are automatically carried over in the final ballot. Only members of the applicable ballot pools can cast a vote. Ballot pool members who previously voted have the option to change their vote in the final ballot. Ballot pool members who did not cast a vote during the previous ballot can vote in the final ballot.

Members of the ballot pools associated with this project can log in and submit their vote for the standard, implementation plan, and definitions here. If you experience any difficulties using the Standards Balloting & Commenting System (SBS), contact Wendy Muller.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The voting results will be posted and announced after the ballots close. If approved, the standard, implementation plan, and definitions will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Standards Development Process

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Al McMeekin (via email) or at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards CIP-003-7(i) FN 2 ST
Voting Start Date: 1/30/2017 11:40:41 AM
Voting End Date: 2/8/2017 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 2
Total # Votes: 316
Total Ballot Pool: 365
Quorum: 86.58
Weighted Segment Value: 78.55

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	91	1	63	0.818	14	0.182	0	3	11
Segment: 2	7	0.2	1	0.1	1	0.1	0	3	2
Segment: 3	79	1	52	0.788	14	0.212	0	2	11
Segment: 4	27	1	16	0.696	7	0.304	0	0	4
Segment: 5	87	1	56	0.778	16	0.222	0	2	13
Segment: 6	57	1	40	0.769	12	0.231	0	1	4
Segment: 7	3	0.1	1	0.1	0	0	0	0	2
Segment: 8	3	0.3	3	0.3	0	0	0	0	0
Segment: 9	2	0.1	0	0	1	0.1	0	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.6	6	0.6	0	0	0	2	1
Totals:	365	6.3	238	4.949	65	1.351	0	13	49

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		Affirmative	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		None	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Devin Elverdi		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Negative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	N/A
1	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Negative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Negative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Negative	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry Bllke		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	N/A
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		None	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Negative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Kissimmee Utility Authority	Anthony Darnell		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Negative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Abstain	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Negative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		Affirmative	N/A
4	Austin Energy	Tina Garvey		Negative	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	N/A
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Negative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	LaGen	Richard Comeaux		Negative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Jeanie Doty		Negative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Cowlitz County PUD	Ron Sporseen		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		Negative	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Negative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	N/A
5	Lakeland Electric	Jim Howard		Negative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		None	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Negative	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Negative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Negative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer	Tim Womack	Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Santee Cooper	Tommy Curtis		Negative	N/A
5	Seattle City Light	Mike Haynes		Negative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Negative	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons		Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Negative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		None	N/A
6	Entergy	Julie Hall		Negative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Negative	N/A
6	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	N/A
6	Omaha Public Power District	Joel Robles		Negative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Negative	N/A
6	Seattle City Light	Charles Freeman		Negative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		None	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Abstain	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 365 of 365 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards CIP-003-7(i) Implementation Plan FN 2 OT
Voting Start Date: 1/30/2017 11:42:20 AM
Voting End Date: 2/8/2017 8:00:00 PM
Ballot Type: OT
Ballot Activity: FN
Ballot Series: 2
Total # Votes: 312
Total Ballot Pool: 365
Quorum: 85.48
Weighted Segment Value: 86

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	91	1	64	0.842	12	0.158	0	3	12
Segment: 2	7	0.1	1	0.1	0	0	0	4	2
Segment: 3	79	1	57	0.864	9	0.136	0	2	11
Segment: 4	27	1	18	0.818	4	0.182	0	1	4
Segment: 5	87	1	60	0.845	11	0.155	0	2	14
Segment: 6	57	1	44	0.863	7	0.137	0	1	5
Segment: 7	3	0.1	1	0.1	0	0	0	0	2
Segment: 8	3	0.3	3	0.3	0	0	0	0	0
Segment: 9	2	0.1	0	0	1	0.1	0	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.6	6	0.6	0	0	0	1	2
Totals:	365	6.2	254	5.332	44	0.868	0	14	53

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		None	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Devin Elverdi		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Negative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Negative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	N/A
1	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Negative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Negative	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry Bllke		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		None	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Kissimmee Utility Authority	Anthony Darnell		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Negative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Abstain	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		Affirmative	N/A
4	Austin Energy	Tina Garvey		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	N/A
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Negative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seminole Electric Cooperative, Inc.	Michael Ward		Affirmative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Cowlitz County PUD	Ron Sporseen		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		Negative	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Affirmative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	N/A
5	Lakeland Electric	Jim Howard		Negative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		None	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Negative	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Negative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer	Tim Womack	Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Santee Cooper	Tommy Curtis		Negative	N/A
5	Seattle City Light	Mike Haynes		Negative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Negative	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons		Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		None	N/A
6	Entergy	Julie Hall		Negative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Negative	N/A
6	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Negative	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		None	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 365 of 365 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards Transient Cyber Asset | New Definition FN 2 DEF
Voting Start Date: 1/30/2017 11:41:20 AM
Voting End Date: 2/8/2017 8:00:00 PM
Ballot Type: DEF
Ballot Activity: FN
Ballot Series: 2
Total # Votes: 314
Total Ballot Pool: 365
Quorum: 86.03
Weighted Segment Value: 85.81

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	91	1	66	0.868	10	0.132	0	3	12
Segment: 2	7	0.1	1	0.1	0	0	0	4	2
Segment: 3	79	1	57	0.864	9	0.136	0	2	11
Segment: 4	27	1	18	0.783	5	0.217	0	0	4
Segment: 5	87	1	61	0.859	10	0.141	0	2	14
Segment: 6	57	1	44	0.846	8	0.154	0	1	4
Segment: 7	3	0.1	1	0.1	0	0	0	0	2
Segment: 8	3	0.3	3	0.3	0	0	0	0	0
Segment: 9	2	0.1	0	0	1	0.1	0	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.6	6	0.6	0	0	0	2	1
Totals:	365	6.2	257	5.32	43	0.88	0	14	51

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		None	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Devin Elverdi		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Negative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	N/A
1	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Negative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry Bllke		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		None	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Negative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Kissimmee Utility Authority	Anthony Darnell		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Negative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Abstain	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Negative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		Affirmative	N/A
4	Austin Energy	Tina Garvey		Negative	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	N/A
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Negative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seminole Electric Cooperative, Inc.	Michael Ward		Affirmative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Cowlitz County PUD	Ron Sporseen		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		Negative	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Negative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	N/A
5	Lakeland Electric	Jim Howard		Negative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		None	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Negative	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer	Tim Womack	Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Santee Cooper	Tommy Curtis		Negative	N/A
5	Seattle City Light	Mike Haynes		Negative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons		Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Negative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		None	N/A
6	Entergy	Julie Hall		Negative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Negative	N/A
6	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Negative	N/A
6	Seattle City Light	Charles Freeman		Negative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Affirmative	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		None	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Abstain	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 365 of 365 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards Removable Media | New Definition FN 2 DEF
Voting Start Date: 1/30/2017 11:41:47 AM
Voting End Date: 2/8/2017 8:00:00 PM
Ballot Type: DEF
Ballot Activity: FN
Ballot Series: 2
Total # Votes: 312
Total Ballot Pool: 365
Quorum: 85.48
Weighted Segment Value: 85.54

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	91	1	66	0.868	10	0.132	0	3	12
Segment: 2	7	0.1	1	0.1	0	0	0	4	2
Segment: 3	79	1	57	0.864	9	0.136	0	2	11
Segment: 4	27	1	18	0.783	5	0.217	0	0	4
Segment: 5	87	1	59	0.843	11	0.157	0	2	15
Segment: 6	57	1	44	0.846	8	0.154	0	1	4
Segment: 7	3	0.1	1	0.1	0	0	0	0	2
Segment: 8	3	0.3	3	0.3	0	0	0	0	0
Segment: 9	2	0.1	0	0	1	0.1	0	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	9	0.6	6	0.6	0	0	0	1	2
Totals:	365	6.2	255	5.304	44	0.896	0	13	53

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Bryan Cox	Rich Hydzik	None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		None	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Devin Elverdi		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Negative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Empire District Electric Co.	Ralph Meyer		None	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	William Smith		Affirmative	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	N/A
1	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Justin Wilderness		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Negative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	Midcontinent ISO, Inc.	Terry Bllke		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Aaron Austin		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	Anaheim Public Utilities Dept.	Dennis Schmidt		None	N/A
3	APS - Arizona Public Service Co.	Jeri Freimuth		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Negative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Kissimmee Utility Authority	Anthony Darnell		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		Negative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Abstain	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Okanogan County	Dale Dunckel		None	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Negative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		Affirmative	N/A
4	Austin Energy	Tina Garvey		Negative	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Julie Hegedus		None	N/A
4	DTE Energy - Detroit Edison Company	Daniel Herring		None	N/A
4	FirstEnergy - Ohio Edison Company	Doug Hohlbaugh		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	N/A
4	Fort Pierce Utilities Authority	Thomas Parker	Chris Gowder	Negative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seminole Electric Cooperative, Inc.	Michael Ward		Affirmative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Jeanie Doty		Negative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Affirmative	N/A
5	Black Hills Corporation	George Tatar		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Affirmative	N/A
5	Cowlitz County PUD	Ron Sporseen		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Empire District Electric Co.	Michael kidwell		None	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		Negative	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Roger Dufresne		Negative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	N/A
5	Lakeland Electric	Jim Howard		Negative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		None	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Negative	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Pacific Gas and Electric Company	Alex Chua		None	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Lynda Kupfer	Tim Womack	Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Santee Cooper	Tommy Curtis		Negative	N/A
5	Seattle City Light	Mike Haynes		Negative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tallahassee Electric (City of Tallahassee, FL)	Karen Webb		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons		Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Negative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		None	N/A
6	Entergy	Julie Hall		Negative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Negative	N/A
6	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Negative	N/A
6	Seattle City Light	Charles Freeman		Negative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Affirmative	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		None	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		None	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 365 of 365 entries

Exhibit H

Standard Drafting Team Roster

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Drafting Team Roster

Project 2016-02 Modifications to CIP Standards

	Name	Entity
Co-Chair	Christine Hasha	Electric Reliability Council of Texas
Co-Chair	David Revill	Georgia Transmission Corporation
Members	Steven Brain	Dominion
	Jay Cribb	Southern Company
	Jennifer Flandermeyer	Kansas City Power and Light
	Tom Foster	PJM Interconnection
	Richard Kinas	Orlando Utilities Commission
	Forrest Krigbaum	Bonneville Power Administration
	Philippe Labrosse	Hydro-Quebec TransEnergie
	Mark Riley	Associated Electric Cooperative, Inc.
PMOS Liaison	Brian Murphy	NextEra Energy
	Andrew Gallo	Austin Energy