Standard Development Timeline

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

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for an additional comment period and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period and Ballot	~~September~~ November 2014
Final Ballot is Conducted	~~October/November 2014~~January 2015
Board of Trustees (Board) Adoption	~~November 2014~~February 2015
Filing to Applicable Regulatory Authorities	~~December 2014~~February 2015

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~~	~~June 2014~~	~~Responding to FERC Order No. 791.~~	~~Revised~~
6	11/13/14	Adopted by the NERC Board of Trustees.	

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

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 ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~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 ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~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:

~~Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R1, Part 1.2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 1 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 2 until the later of April 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 3 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 4 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.~~ 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 ~~a minimum level of~~ 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, ~~and~~ medium, and low impact BES Cyber Systems. For example, a single ~~training~~ cyber security awareness program could meet the requirements for training personnel 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 ~~Bulk Electric System~~BES. A review of UFLS tolerances defined within ~~regional~~ Regional ~~reliability~~ Reliability ~~standards~~ 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

Rationale for Requirement R1:

One or more security policies enable effective implementation of the ~~standard's~~ 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 ~~its~~ 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 ~~standard's~~ requirements.

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

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~~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.

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 ~~The requirement to implement a cyber security plan~~ for assets containing low impact BES Cyber Systems. ~~provides a minimum set of cyber security controls for assets containing low impact BES Cyber Systems. Individually, these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised. To that end,~~ The ~~Requirement R2 requires Responsible Entities to implement documented~~ cyber security plan(s) ~~covering~~ covers four subject matter areas: ~~–~~ (1) cyber security awareness~~,~~; (2) physical ~~access~~ security controls~~,~~; (3) electronic access controls~~,~~; and (4) ~~cyber~~ Cyber ~~security~~ Security ~~incident~~ Incident response. ~~In response to directives in FERC Order No. 791, Requirement R2 provides for the specific elements that must be included in the cyber security plan(s). Attachment 1 provides these elements. These~~ This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for ~~sufficient~~ operational, procedural, and technical safeguards for ~~assets containing~~ low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the ~~Bulk Power System~~BES, Attachment 1 provides Responsible Entities flexibility on how to apply the ~~required~~ security controls to meet the security objectives. Additionally, ~~the SDT recognizes that~~because many Responsible Entities have ~~multiple~~ multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their ~~and has provided the ability to use~~ 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, ~~the objective criteria within~~ Attachment 1.

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

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 ~~elements~~ 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 ~~elements~~ sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per ~~element~~ section are located in Attachment 2.

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~~ Senior ~~manager~~ Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

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.

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.

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~~7, Requirement R2, Attachment 1, ~~element~~ Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low	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~~7, Requirement R2, Attachment 1, ~~element~~ Section 1. (R2) OR The Responsible Entity documented	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 test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ 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~~7, Requirement R2, Attachment 1. (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 one or more Cyber Security Incident response plans according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 4. (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 update each Cyber Security Incident response plan(s) within 180 days according to CIP-003-7,	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, classification, and response to Cyber Security Incidents according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 4. (R2) ~~OR~~ ~~The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing~~	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-ISAC) according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 4. (R2) OR The Responsible Entity documented and implemented electronic access controls for ~~Low Impact External Routable Connectivity~~LERC, but failed to ~~establish~~ implement a ~~Low Impact Electronic Access Point~~LEAP~~,~~ or permit inbound and outbound access ~~and deny all other access, or other electronic access~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R2, Attachment 1, Section 4. (R2)	~~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, element 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	~~controls that provide equal or greater level of protection~~ according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ 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-003-7, Requirement R2, Attachment 1, ~~element~~ Section 3. (R2) OR	

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 (ES-ISAC) according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ 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 ~~access~~ security controls according to CIP-003-~~6~~7, Requirement R2, Attachment 1, ~~element~~ Section 2. (R2)	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical ~~access~~ security controls according to CIP-003-7, Requirement R2, Attachment 1, ~~element~~ Section 2. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				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~~7, Requirement R2, Attachment 1, ~~element~~ 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	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	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 The Responsible Entity has identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change in less than 40 calendar days of the change. (R3)	document this change in less than 50 calendar days of the change. (R3)	less than 60 calendar days of the change. (R3)	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 specific actions delegated, but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						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.

CIP-003-~~6~~ 7 - Attachment 1

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

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

Responsible Entities with ~~multiple~~ multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the ~~elements~~ 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 S~~s~~ecurity ~~awareness~~Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, ~~its~~ cyber security practices (which may include associated physical security practices)~~, using one or a combination of the following methods:~~

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

Section 2. Physical ~~access s~~Security ~~controls~~Controls: Each Responsible Entity shall ~~implement controls to restrict~~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.~~, based on need as determined by the Responsible Entity, through one or more of the following:~~

- ~~Access controls;~~
- ~~Monitoring controls; or~~

~~Other operational, procedural, or technical physical security controls.~~

Section 3. Electronic ~~access~~ Access C~~c~~ontrols: Each Responsible Entity shall ~~implement controls to restrict electronic access for Low Impact External Routable Connectivity and Dial-up Connectivity, which shall include the following, or other electronic access controls that provide an equal or greater level of protection~~:

3.1 For ~~any Low Impact External Routable Connectivity~~LERC, if any, ~~establish~~ implement a ~~Low Impact BES Cyber System Electronic Access Point~~ LEAP ~~that~~ to permit~~s~~ only necessary inbound and outbound bi-directional routable protocol access ~~and denies all other access~~; and

~~**3.2** Authentication~~ Implement authentication ~~of~~ for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

~~**3.2**~~

3.2

Section 4. Cyber Security Incident ~~response~~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-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

~~Record retention related to Reportable Cyber Security Incidents.~~

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~~ 7 - Attachment 2

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

~~Element~~ Section 1 - Cyber ~~security~~ Security ~~awareness~~Awareness: An example of evidence for ~~element~~ 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 ~~has been provided~~ through one or more of the following methods: ~~dated copies of the information used to reinforce security awareness via direct communications, indirect communications or management support and reinforcement.~~

- 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).

~~Element~~ Section 2 - Physical ~~s~~Security ~~c~~Controls: Examples of evidence~~s~~ for ~~element~~ Section 2 may include, but are not limited to:

- Documentation of the selected ~~one or more~~ access control(s) (e.g., card key, ~~special~~ locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls ~~to restrict~~ 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 the ~~Low Impact BES Cyber System Electronic Access Point~~LEAP.
    ~~c.~~b. ~~Documentation showing that the physical access restrictions cited above are based on need, which may include, but is not limited to, a policy describing the high level operational or business need(s) for physical access.~~

~~Element~~ Section 3 - Electronic ~~a~~Access ~~c~~Controls: Examples of evidence for ~~element~~ Section 3 may include, but are not limited to:

- Documentation showing that inbound and outbound connections ~~(e.g. IP addresses, ports, services)~~ for any ~~Low Impact BES Cyber System Electronic Access Point~~LEAP 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).~~; or~~
- ~~Documentation of other electronic access controls that provide an equal or greater level of protection.~~

~~Element~~ Section 4 - Cyber Security Incident ~~r~~Response: An example of evidence for ~~element~~ 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~~ Incident and for notifying the Electricity Sector Information Sharing and Analysis Center (ES-ISAC);
2. ~~the~~ to ~~identification~~ identify and document~~ation of~~ the roles and responsibilities for Cyber Security Incident response by groups of 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 retain records related to Reportable Cyber Security Incidents (e.g., security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes).~~

~~6.~~5. to update, as needed, ~~Also include dated revised~~ Cyber Security Incident response plan(s) ~~that identify that the plan(s) were updated~~ within 180 calendar days after ~~a~~ 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~~ the number of policies and their ~~specific language~~content ~~are~~ 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. ~~If a Responsible Entity has any high or medium impact BES Cyber Systems, the cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-6, Requirement R1.1. If a Responsible Entity has any assets from CIP-002 containing low impact BES Cyber Systems, the cyber security policy must cover in sufficient detail the four topical areas required by Requirement R1.2.~~ The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering ~~these~~ 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-003-7, 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.

~~For~~ Responsible Entities that have ~~multiple~~ multiple-impact rated BES Cyber Systems~~, they~~ are not required to create separate cyber security policies for high~~, or~~ medium~~, and~~ 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-~~004~~ 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~~from CIP-004 through CIP-011~~, but ~~rather to put together~~to develop a holistic cyber security policy appropriate ~~to~~ for its organization. ~~The assessment through the Compliance Monitoring and Enforcement Program of~~ Elements of a policy ~~items~~ that extend beyond the scope of ~~CIP-004 through CIP-011~~NERC's cyber security Reliability Standards ~~should~~ 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, ~~T~~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~~policy~~:

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

~~The Standard Drafting Team (SDT) has removed r~~Requirements relating to exceptions to a Responsible Entity's security policies were removed ~~since~~ because it is a general management issue that is not within the scope of a reliability requirement. ~~The SDT considers i~~It ~~to be~~is an internal policy requirement and not a reliability requirement. However, ~~the SDT encourages~~

Responsible Entities are encouraged to continue this practice as a component of ~~its~~ their cyber security ~~policy~~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 ~~all~~ low impact BES Cyber Systems. The ~~SDT is~~ 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~~balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do meet the definition of having a 15-minute adverse impact so some protections are needed~~.~~ The intent is that ~~such~~ 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 ~~main~~ subject matter areas, as ~~detailed~~ identified in Attachment 1, that must be covered by ~~this~~ the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for ~~Low Impact External Routable Connectivity~~LERC and Dial-up Connectivity, and ~~cyber security incident~~(4) Cyber Security Incident response.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the ~~elements~~ sections that must be in the cyber security plan(s). The ~~SDT's~~ 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 ~~and not~~ rather than maintain two separate programs. Guidance for each of the ~~4~~ 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. ~~It is up to t~~The entity ~~as to~~has the discretion to determine the topics to be addressed and ~~how it~~the manner in which it will communicate ~~schedules~~ these topics. ~~The~~ As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered ~~and~~ according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.)~~ that were used~~. The ~~SDT does not intend that the~~ Responsible Entity ~~must~~ 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 ~~used~~ 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 ~~controls~~ methods to ~~restrict~~ control physical access to (1) ~~the~~ low impact BES Cyber Systems at ~~a BES~~ assets containing low impact BES Cyber System(s) and (2) ~~Low Impact BES Cyber System Electronic Access Points~~ LEAPs, if any ~~(see Electronic Access Controls section below)~~. If the LEAP is located within the BES asset and inherits the same controls outlined in ~~element~~ 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. ~~If the LEAP is located at another location, possibly a location without any BES Cyber Systems, then separate documentation and implementation of the physical security controls of the LEAP are required.~~

The Responsible Entity has the flexibility in the ~~controls~~ selection of the methods used to meet the objective to ~~restrict~~ control physical access to the asset(s) containing low impact BES Cyber Systems ~~at a~~or the low impact BES ~~asset~~ Cyber System itself or LEAPs, if any.~~,~~ The Responsible Entity may ~~using~~ use one or a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may ~~utilize~~ use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) ~~and/~~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 would help meet the security objective.

The objective is to ~~restrict~~ control the physical access based on need ~~and~~ as determined by the Responsible Entity. ~~t~~The need can be ~~established~~ documented at the policy level ~~based on higher level operational or business needs~~ for access to the site or systems. ~~The SDT intent is that this need at the higher level be documented such that the requirement cannot be interpreted to mean that any and all access must be restricted.~~ The requirement does not ~~imply that a~~ obligate an entity to ~~specific~~ specify a ~~business~~ need ~~must be documented~~ 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: (~~i~~1) alarm systems to detect motion or entry into a controlled area, or (~~ii~~2) human observation of a controlled area. Monitoring does not necessarily ~~imply~~ 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 ~~as determined by the entity's controls~~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 or Dial-up Connectivity, the Responsible Entity can document the absence of the communication within its low impact cyber security plan.

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 even though there technically is LERC. 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.~~Where Low Impact External Routable Connectivity (LERC) or Dial-up Connectivity exists, the Responsible Entity must document and implement controls that include the LERC and Dial-up Connectivity to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. Two glossary terms are included in order to help clarify and simplify the language in Attachment 1. The SDT's intent in creating these terms is to avoid confusion with the similar concepts and requirements (ESP, EAP, ERC, EACMS) needed for high and medium impact BES Cyber Systems by utilizing separate terms that apply only to assets containing low impact BES Cyber Systems.~~

~~**Low Impact External Routable Connectivity (LERC) –** includes any bi-directional routable protocol based connectivity between low impact BES Cyber Systems within a BES asset and Cyber Assets outside the BES asset containing the low impact BES Cyber Systems. The SDT, in order to avoid future technology issues, is specifically excluding from the definition direct Intelligent Electronic Device (IED) to IED communication used for protection and/or control between low impact BES Cyber Systems at different BES assets, such as IEC 61850 messaging. The SDT does not intend for the requirement to have an electronic access point even though there is LERC or to preclude the use of such time-sensitive (for example 4 ms or less) reliability enhancing functions if they use a routable protocol in the future.~~

~~**Low Impact BES Cyber System Electronic Access Point (LEAP) –**~~ 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. 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 from or to the low impact BES Cyber System.

When identifying a LEAP, Responsible Entities are provided flexibility in the selection of~~is~~ the interface on a Cyber Asset that ~~allows and~~ 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~~a~~ firewall, the internal interface on a router that has implemented an access control list (ACL), or ~~an internal interface on a unidirectional gateway that physically enforces outbound-only data flows~~other security device. ~~LEAP are not to be considered EACMS or meet EACMS specific requirements (as utilized for the Electronic Security Perimeter protecting high and medium impact BES Cyber Systems). However they are required, as per element 2 of the cyber security plan elements, to have physical security controls.~~ The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required ~~is not prescriptive and does not have~~ to reside at the ~~BES~~ asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish~~. This flexibility is included so that the standard does not~~ nor ~~require~~ a unique physical LEAP per ~~BES asset. Responsible Entities can have a single LEAP that controls the LERC from more than one BES~~ 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. ~~However the LERC between assets "behind" the LEAP and another asset containing a low impact BES Cyber System must also pass through the single LEAP.~~ Locating the ~~LEAP~~ Cyber Asset with multiple LEAPs at an external location with multiple ~~BES~~ assets containing low impact BES Cyber Systems "behind" it, however, should not allow ~~unfettered~~ uncontrolled access from one ~~BES~~ asset to all other ~~BES~~ assets sharing the LEAP. ~~It is also not the intent of the SDT where low impact BES Cyber Systems do not have any LERC that additional connectivity be established nor that a LEAP be established.~~

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.

~~The electronic access controls should address the risk of using the asset's LERC or Dial-up Connectivity to gain access to the low impact BES Cyber Systems. For LERC, a LEAP shall be~~

~~implemented that permits only necessary inbound and outbound access and denies all other access.~~

Examples of sufficient access controls may include:

- Any LERC for the asset passes through a LEAP ~~that denies all traffic by default~~ 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) ~~for scenarios representative of the Responsible Entity's sites having Low Impact BES Cyber Systems~~.
- 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.

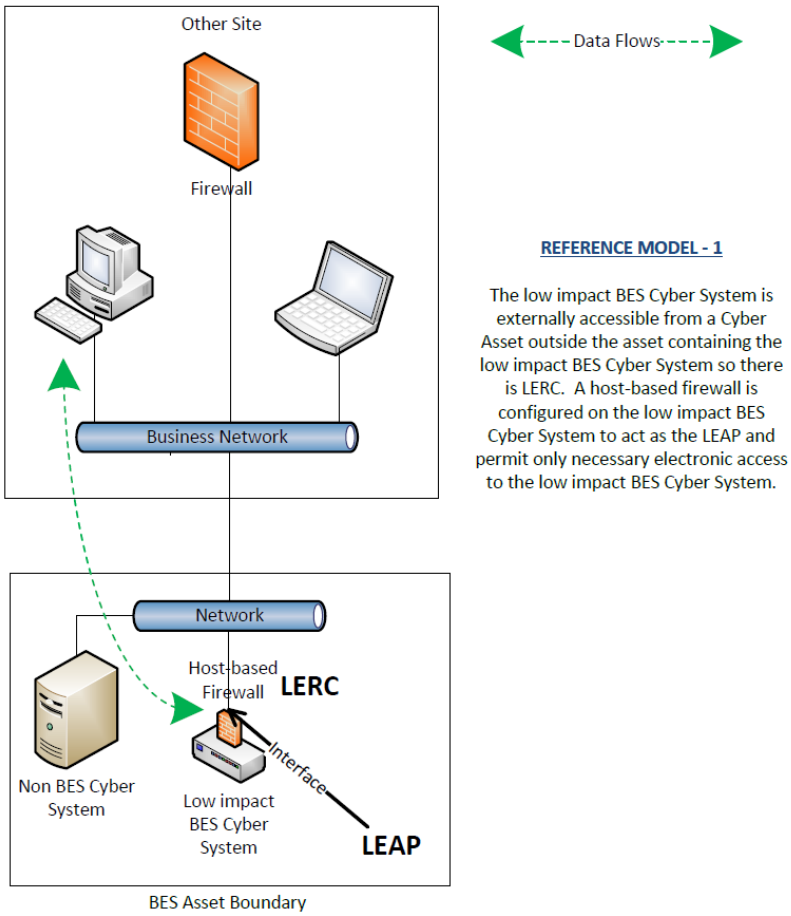
Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

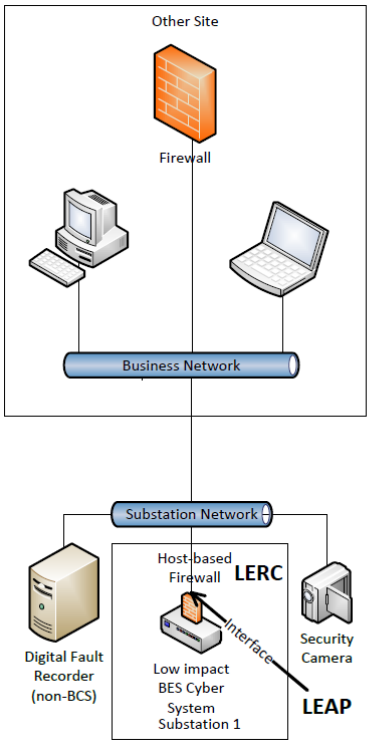
- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- An asset has ~~external routable connectivity~~LERC due to a BES Cyber System within it having a 3G/4G wireless card on a public carrier ~~which~~ 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 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 to depict the rationale for identifying 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.~~The SDT also notes it uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.~~

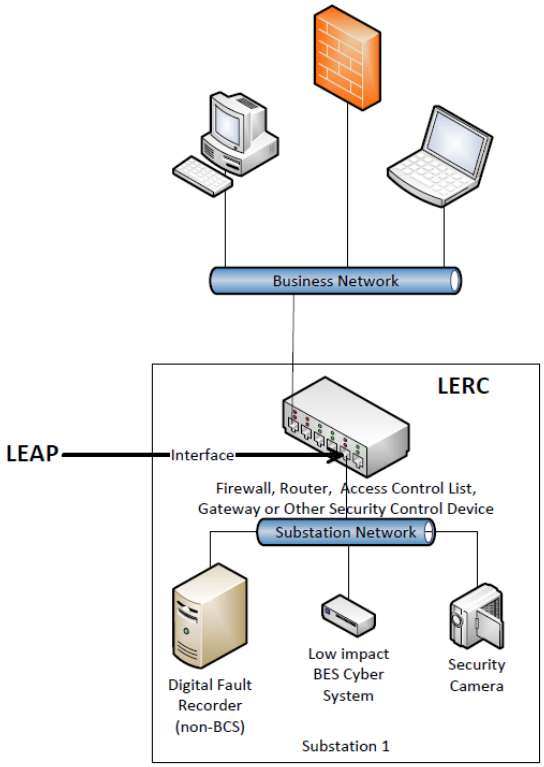
~~The following diagrams explain the SDT's rationale.~~





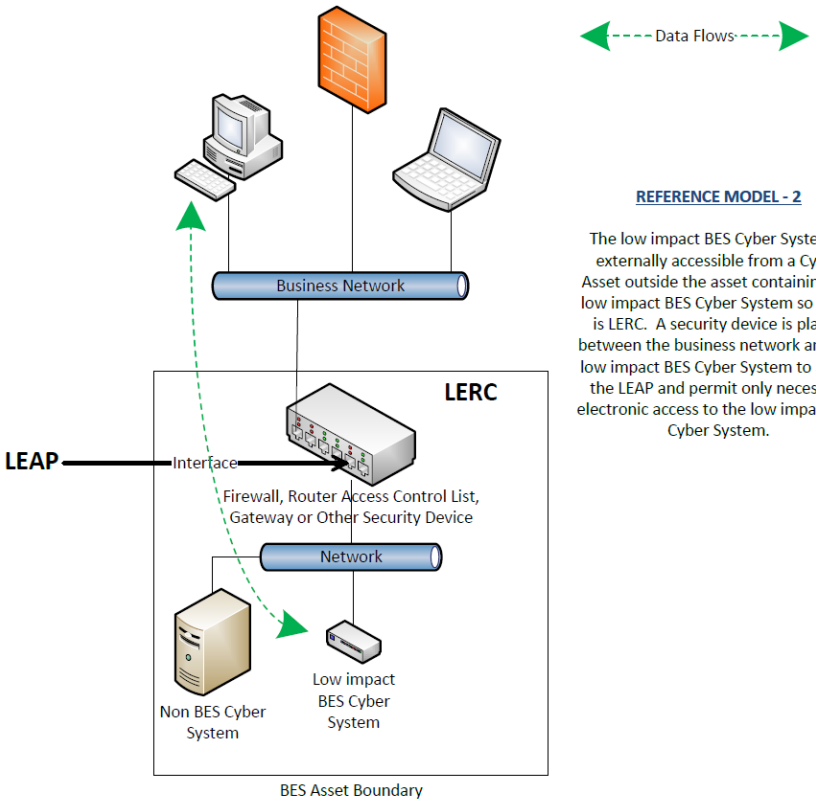
REFERENCE MODEL - 1

The low impact BES Cyber System is behind a LEAP. In this example, the LEAP is the network interface on the low impact BES Cyber System. The host-based firewall restricts electronic access for Low Impact External Routable Connectivity (LERC).



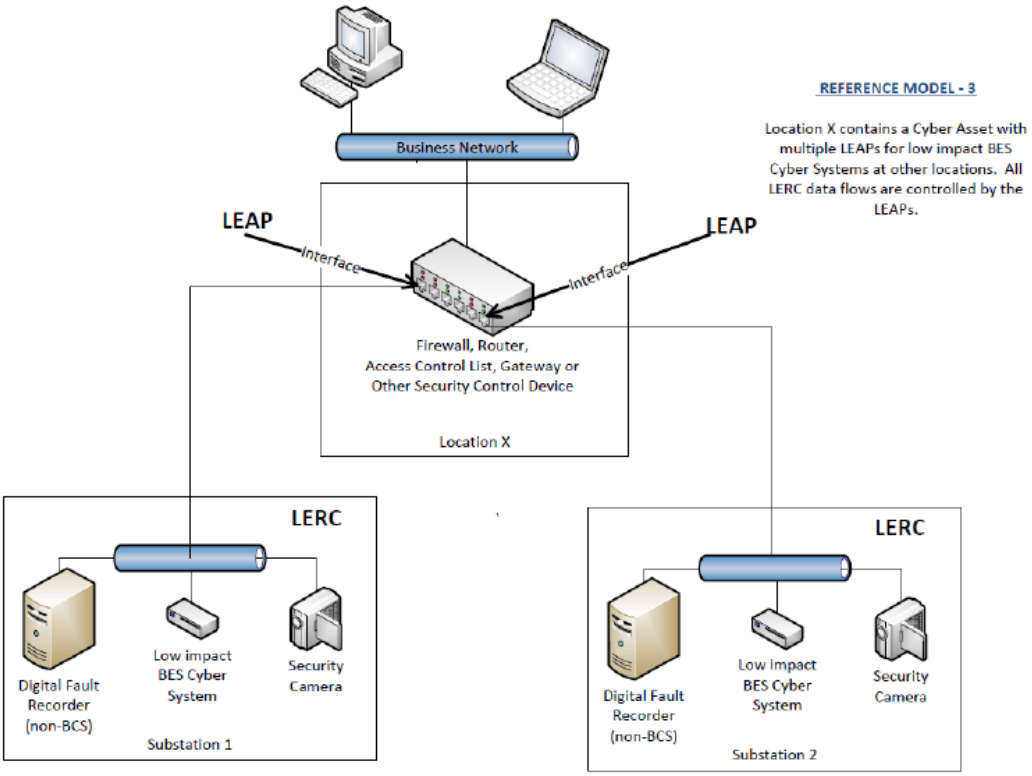
REFERENCE MODEL - 2

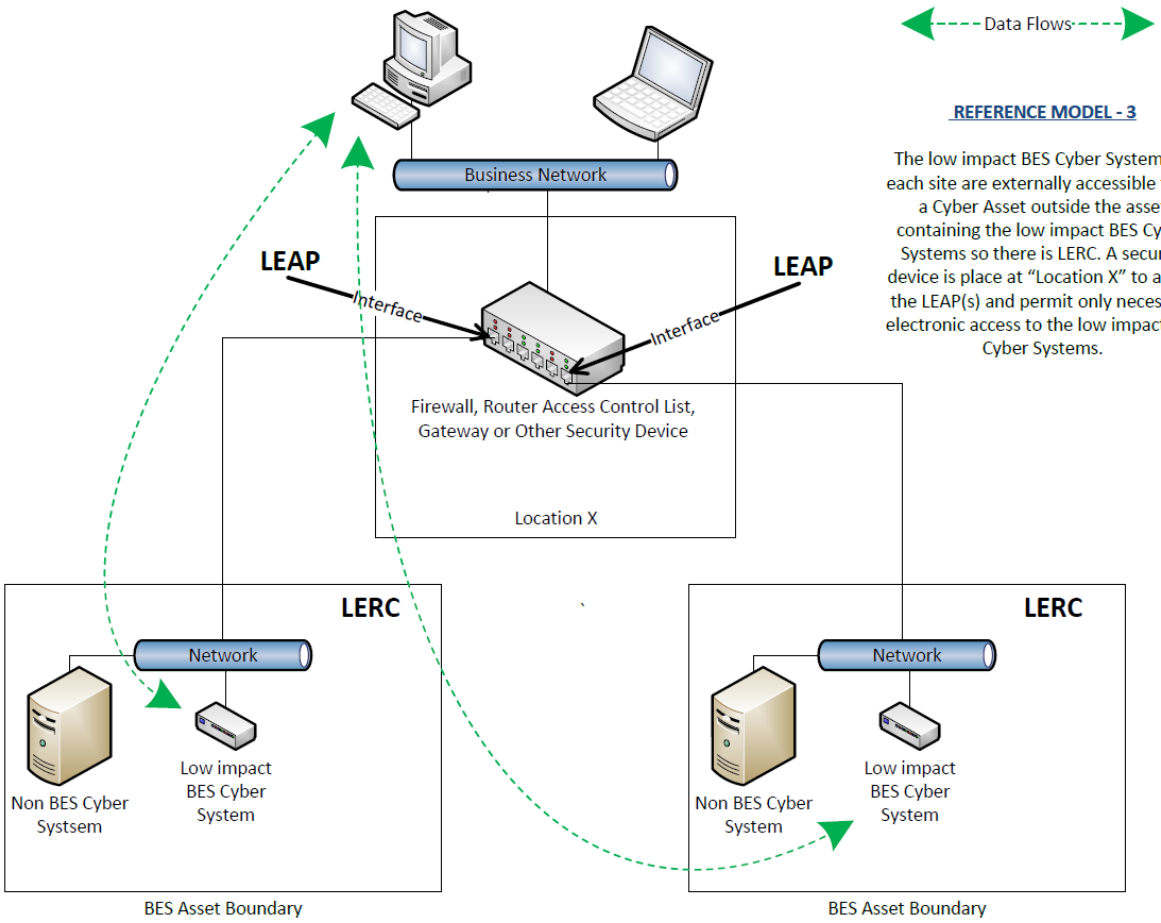
All LERC to the low impact BES Cyber System is controlled by an LEAP.

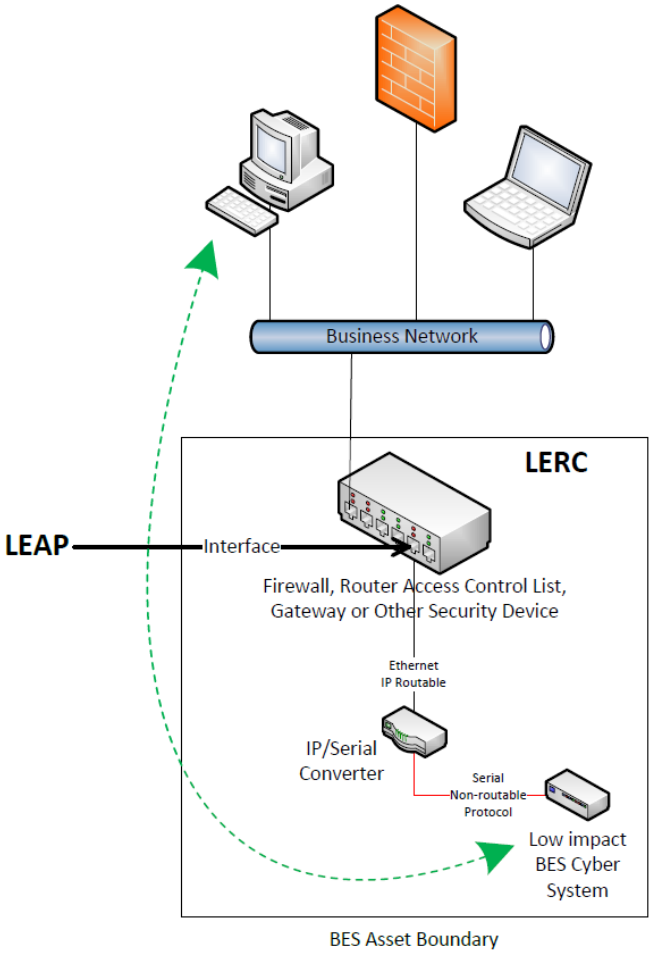


REFERENCE MODEL - 2

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.


REFERENCE MODEL - 3
Location X contains a Cyber Asset with multiple LEAPs for low impact BES Cyber Systems at other locations. All LERC data flows are controlled by the LEAPs.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router, Access Control List, Gateway or Other Security Control Device
Location X
LERC
Digital Fault Recorder (non-BCS)
Low impact BES Cyber System
Security Camera
Substation 1
LERC
Digital Fault Recorder (non-BCS)
Low impact BES Cyber System
Security Camera
Substation 2

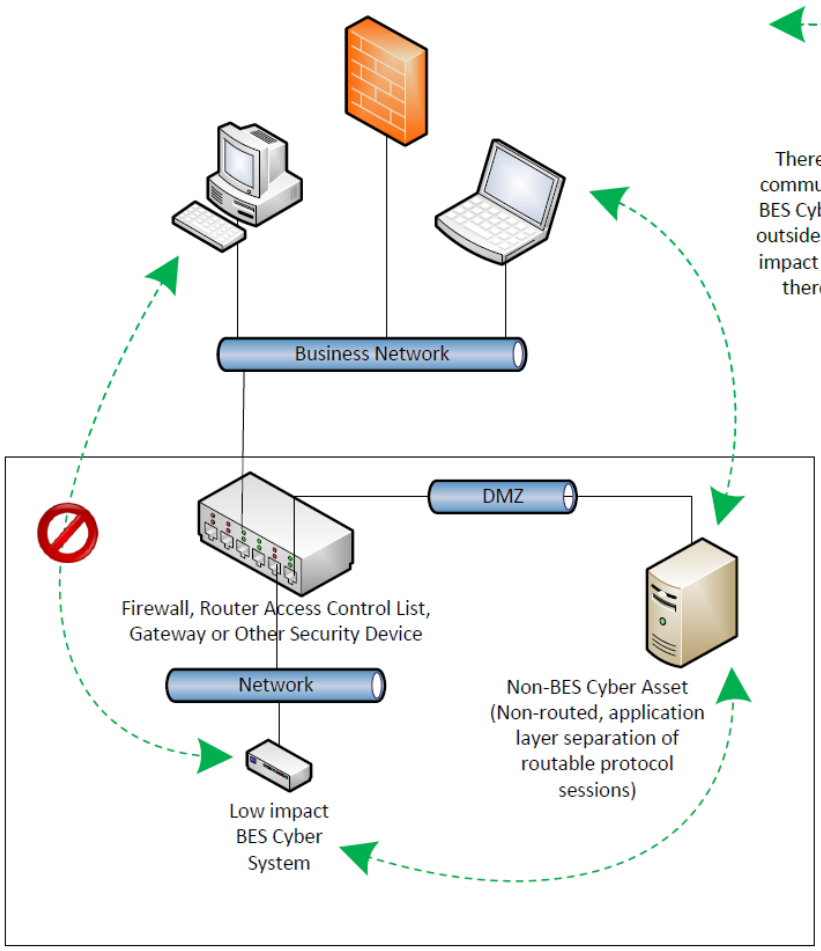

Data Flows
REFERENCE MODEL - 3
The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is place at "Location X" to act as the LEAP(s) and permit only necessary electronic 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

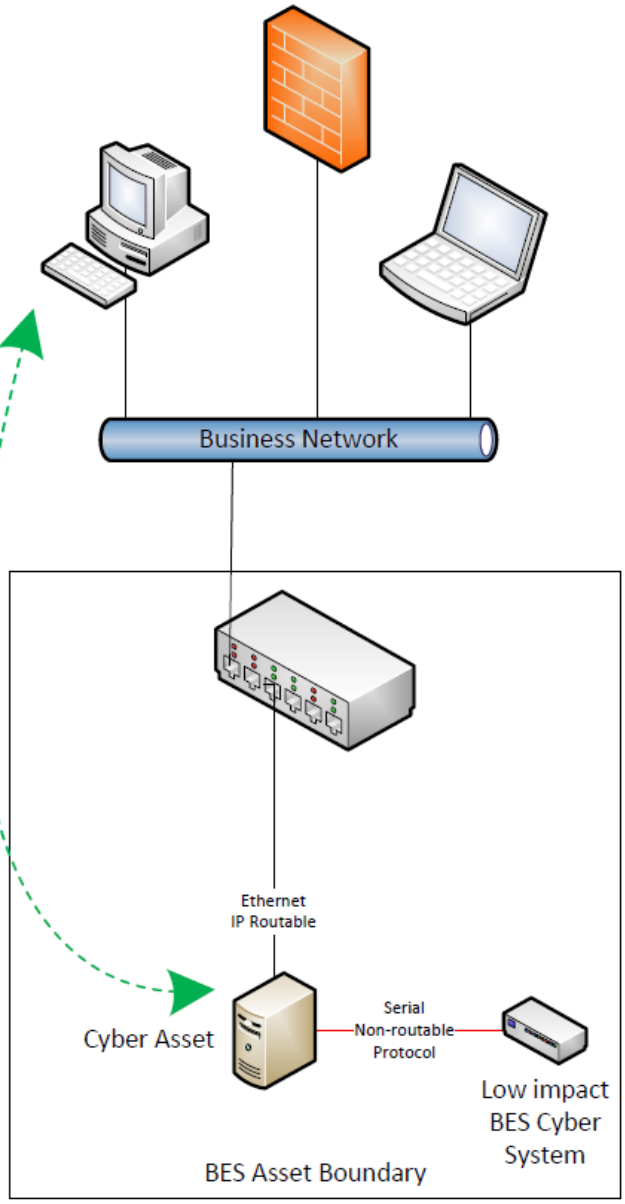


Data Flows

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.

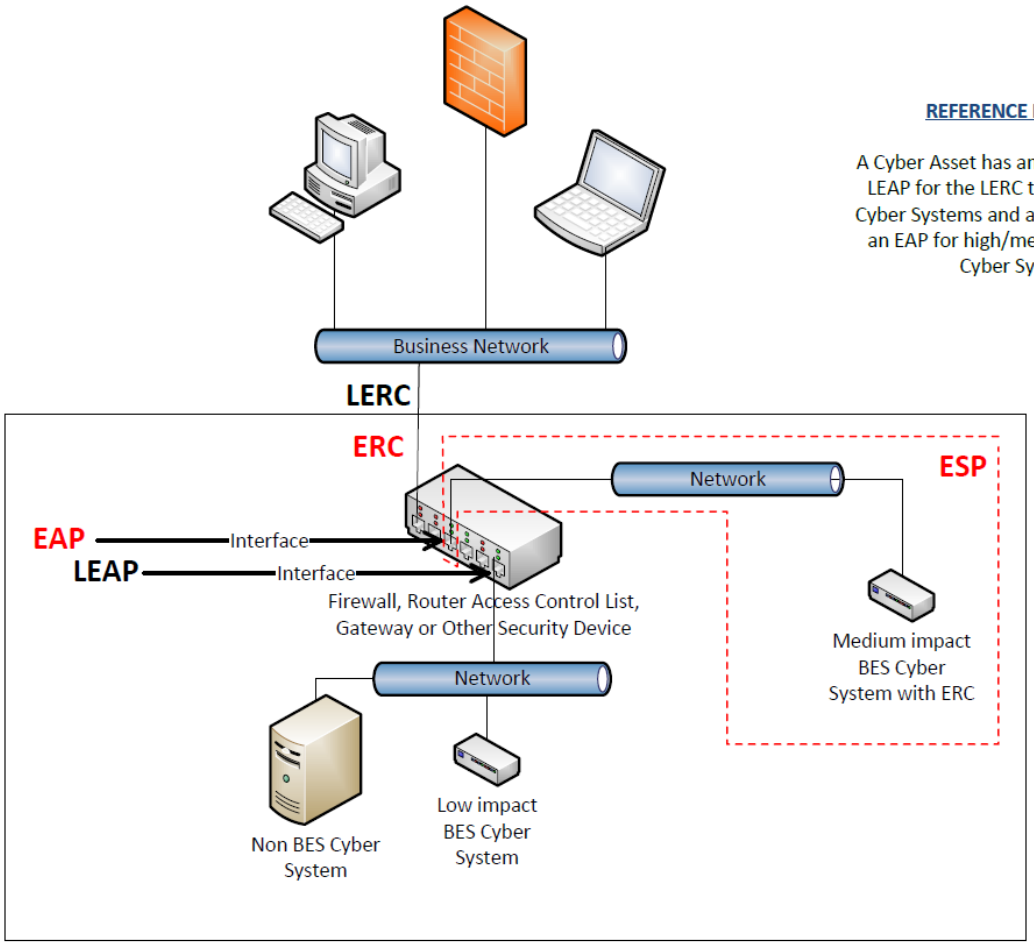

Data Flows
REFERENCE MODEL - 5
There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.
Business Network
DMZ
Firewall, Router Access Control 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~~ Cyber ~~security~~ Security ~~incident~~ Incident response plan(s) that include each of the topics listed in Section 4. ~~For assets that do not have LERC, it is not the intent to increase their risk by increasing the level of connectivity in order to have real-time monitoring. The intent is i~~If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber Systems, the intent is for the entity to implement ~~there is~~ a ~~cyber~~ Cyber ~~security~~ Security ~~incident~~ Incident response plan that will guide the entity ~~through~~ 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 ~~well as~~do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise ~~if~~ provided the entity's response plan is followed. ~~It is the intent of the SDT~~The intent of the requirement is for entities to ~~have~~ keep the ~~cyber~~ Cyber ~~security~~ Security ~~incident~~ Incident response plan(s) ~~kept~~ current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

~~In the event of a Reportable Cyber Security Incident, Attachment 1, element 4.6 specifies entities must retain relevant records for Reportable Cyber Security Incidents. Example evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes. Entities should refer to their handling procedures to determine the types of evidence to retain. The evidence retention period for records related to Reportable Cyber Security Incidents is defined in Section C.1.2 of this Standard, which is the same for all requirements in CIP-003-6.~~

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 ~~this~~ 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 ~~should have~~ significant flexibility to adapt this requirement to ~~their~~ 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 ~~provides~~ 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~~ up ~~to~~ 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.