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.