Background Information
On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, Revised Critical Infrastructure Protection Reliability Standards, approving seven CIP Reliability Standards and new or modified definitions. In Order No. 822, the Commission also directed NERC to make certain modifications to those standards and definitions. On March 9, 2016, the NERC Standards Committee authorized the Standards Authorization Request (SAR) to be posted for a 30-day informal comment period from March 23 – April 21, 2016. Based on the comments received, the 2016-02 Modifications to CIP Standards Drafting Team (SDT) made minor revisions to the SAR which was posted for an additional 30-day informal comment period June 1-30, 2016.

In Order 822, the Commission stated:

“73. Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term “direct” as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.”

SDT Approach
In this revision, the terms Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) have been deleted and the requirements for electronic access controls for asset(s) containing low impact BES Cyber Systems simplified so that it is an attribute of a BES asset. The SDT modified the requirements to permit only inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a
Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls, unless that communication meets the exclusion language. The defined term LEAP is no longer necessary because the SDT changed the requirement from requiring a LEAP to requiring electronic access controls. Additionally, since the SDT is removing the term LERC, the exclusion language that was previously in the definition of LERC was integrated into the Attachment 1, Section 3.1 requirement.

Because the proposed modifications to Reliability Standard CIP-003-7 eliminate the need for the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP), NERC is requesting these terms be retired in the associated implementation plan.

Additionally, the SDT:

- revised the associated Lower, Moderate, and High VSLs for Requirement R2 to complement the requirement revisions;
- corrected a mistake in the Severe VSL for Requirement R2;
- made non-substantive changes to the Moderate and High VSLs for Requirement R2 to align with the order of the requirement;
- removed repetitive text from Requirement R1, Part 1.2.3 to make it consistent with Parts 1.2.1 and 1.2.2;
- updated the Guidelines and Technical Basis section of the standard to reflect the revisions made to the Attachments;
- made non-substantive errata changes throughout the standard such as replacing “ES-ISAC” with “E-ISAC”; and
- revised the Implementation Plan to reflect revisions to the draft standard and to provide additional clarity.

The SDT requests feedback on the proposed approach to addressing the FERC directive.
Questions

1. Definition: The SDT is proposing the retirement of the terms Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP). The SDT incorporated the LERC concepts into the Requirement R2 language and removed the LERC reference from Requirement R1, Part 1.2.3 and the LEAP references from Attachment 1, Sections 2 and 3.1. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.
   Yes: X
   No: 
   Comments:

2. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 3 to require each Responsible Entity to implement electronic access controls for each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002 that permit only necessary inbound and outbound electronic access as determined by the Responsible Entity. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.
   Yes: X
   No: 
   Comments:

3. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 2 Physical Security Controls to reflect the retirement of LEAP. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.
   Yes: X
   No: 
   Comments:

4. Attachment 2: The SDT revised the complementary language of CIP-003-6, Attachment 2, Sections 2 and 3 to make the evidential language of the measure consistent with the revised requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.
   Yes: X
   No: 
   Comments:
5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides example diagrams that illustrate various electronic access controls at a conceptual level. Do you agree with the revised content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

Yes: 
No: X

Comments:
The language of several Reference Models states “When permitting the inbound and outbound electronic access permissions, at a minimum, the permissions need to restrict source and destination addresses, or a range of addresses when necessary.” This language sounds like a Requirement. Recommend striking this sentence in all locations because the diagrams should be illustrative, allowing the Responsible Entity Flexibility to implement appropriate security controls, as provided by the Requirements language. Also recommend striking the final sentence in Reference Models 1, 2 and 3. These security controls are good suggestions and could be added as suggestions at the beginning of the Guidelines and Technical Basis.

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) date for the revisions made to CIP-003, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority’s order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer, please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

Yes: 
No: X

Comments:
Due to budget cycles and quantity of equipment that must be installed, we propose keeping the language included in the “General Consideration” section but extend the interval from 12 months to 18 months.

7. If you have additional comments on the proposed revisions to address the FERC directive regarding the LERC definition that you have not provided in response to the questions above, please provide them here.

Comments:
None.