NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard
CIP-003-9 – Low Impact BES Cyber Security Criteria Revisions

Introduction
This document is the technical rationale and justification for Reliability Standard CIP-003-A and includes the rationale for changes in the current proposed version, as well as previous versions of the standard.

It is intended to provide stakeholders and the ERO Enterprise with an understanding of the revisions, technology and technical concepts of Reliability Standard CIP-003-9. This is not a Reliability Standard and should not be considered mandatory and enforceable.

Background
In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts, representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber-attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the Standard Authorization Request (SAR) at its March 22, 2023 meeting.

The LICRT conclusions regarding low impact BES Cyber Systems are as follows:

- Individually, low impact BES Cyber Systems are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the team does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems.
- The team recognizes that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The team recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.

Those LICRT report recommendations are as follows:

- Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity.

Rationale for Attachment 1, Section 3 and Section 6

The Standard Drafting Team's (SDT's) review of the SAR and industry comment initiated a discussion of where the requirements would reside within CIP-003-9. CIP-003-9 was used as the baseline for revisions, since this version is the most recent version approved by FERC. Attachment 1, Section 3 and Attachment 1, Section 6 were identified as ideal locations to integrate the requirements due to their focus on Electronic Access Controls and Vendor Electronic Remote Access Security Controls. The SDT investigated two options:

Option A: Modify Sections 3 and 6; integrating the requirements, but keeping the sections separate
Option B: Merge Sections 3 and 6

The SDT agreed to Option B: Merge Sections 3 and 6. The following rationale was used to support the decision:

1. Merging Section 3 and Section 6 would present a single section for all electronic access with sub-sections providing additional requirements based on the type of access (Vendor, dial-up, local, etc.)
2. Section 6 has not been implemented or required by industry at this time and therefore there would be no impact to merging it with Section 3

While merging Section 3 and 6, the SDT made conforming changes to the language. The SDT uses the phrase "implement controls" to replace "implement a process" or "implement one or more method(s)". The SDT believes a "control" can include an operation, process, procedure, technology as described in the examples of Attachment 2.

Glossary Terms

The SDT also discussed the potential resurrection of the retired NERC Glossary Term: LERC, Low Impact External Routable Connectivity, or creating a new Glossary Term. The rationale for using LERC or a new Glossary Term would be to provide a shorthand way of discussing external routable connectivity when dealing with low impact assets. LERC was initially created by the Project 2014-02 SDT in response to FERC Order 791. FERC Order 822 approved the term but with a directive to address an issue within the definition of the term in 12 months. Project 2016-02 was formed to address the issue and choose to retire the term and integrate the language into Attachment 1, Section 3.1. LERC was only in use between its approval on July 1, 2016 through its retirement on December 31, 2019.

The SDT decided to retain existing CIP-003-9 Section 3.1 rather than resurrect LERC term or create a new Glossary Term. Rationale used for the decision:

1. Possible confusion with reviving LERC
2. Possible friction with stakeholders with creating/using a non-standard/new term
3. The concept of LERC is currently not used outside of CIP-003-A, Section 3

Section 3.1

The objective of Section 3.1 is to maintain the original language used in CIP-003-9, Section 3.1, Subsections (i) - (iii). There is one revision to 3.1(iii) replacing the protocol language with reference to "Protection Systems", which is a conforming change made by Project 2016-02, CIP-003-Y.

Section 3.1.1

The objective of Section 3.1.1 is to maintain the original language used in CIP-003-9, Section 3.1.

Section 3.1.2

This is an expanded cyber security control outlined in the SAR. The scope is expanded from CIP-003-9, Section 6.3 to include all communications rather than vendor specific communications. The objective of Attachment 1 Section 3.1.2 is for entities to mitigate the risk posed by malicious communications to or from low impact BES Cyber Systems. The obligation in Section 3.1.2 requires that entities implement controls to detect known or suspected inbound and outbound malicious communications between a low impact BES Cyber System and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).

Section 3.1.3

This is a new cyber security control outlined in the SAR, which requires entities to implement controls to authenticate users when permitting (allowing) each instance of electronic remote access to networks containing low impact BES Cyber Systems. This intention of "each instance" phrase is meant to include the initial authorization and all subsequent re-connection instances of electronic remote access to the network. If there is a collection of sub-networks or Cyber Assets within the network containing low impact BES Cyber Systems, then multiple re-authentications would not be required. This control mitigates the risk of unauthenticated user access.

Section 3.1.4

This is a new cyber security control outlined in the SAR. The objective of Attachment 1, Section 3.1.4 is for entities to have the ability to protect the user authentication information (username, password, multi-factor authentication (MFA) information, session token, etc.) between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s). This protection mitigates the unintended disclosure of authentication information for remote access of low impact cyber systems.

Section 3.1.5

The objective of Section 3.1.5 is to maintain the original language used in CIP-003-9, Section 6.1. One or more method(s) can be identified as part of this electronic access control. Entities must determine vendor electronic remote access, where permitted, to their low impact BES Asset(s) and/or BES Cyber Systems.

Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access.

Section 3.1.6
The objective of Section 3.1.6 is to maintain the original language used in CIP-003-9, Section 6.2. One or more method(s) can be identified as part of this electronic access control. Entities must have the ability to disable vendor electronic remote access, where permitted, for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing low impact BES Cyber Systems.

Section 3.2
The objective of Section 3.2 is to maintain the original language used in CIP-003-9, Section 3.2.

Rationale for Attachment 2

The SDT made conforming changes to Attachment 2 merging Sections 3 and 6, and providing examples of compliance related activities.

Previous CIP-003 Versions Technical Rationale

Project 2020-03 Supply Chain Low Impact Revisions (CIP-003-9) Technical Rationale

Project 2016-02 Modifications to CIP Standards (CIP-003-Y) Technical Rationale