NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2023-04 Webinar Modifications to CIP-003

Jay Cribb, Southern Company
Joe Chesney, Powder River Energy
Barry Jones, WAPA
November 16, 2023

RELIABILITY | RESILIENCE | SECURITY




Administrative Items

- NERC Antitrust Guidelines
  - It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.
- Notice of Open Meeting
  - Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

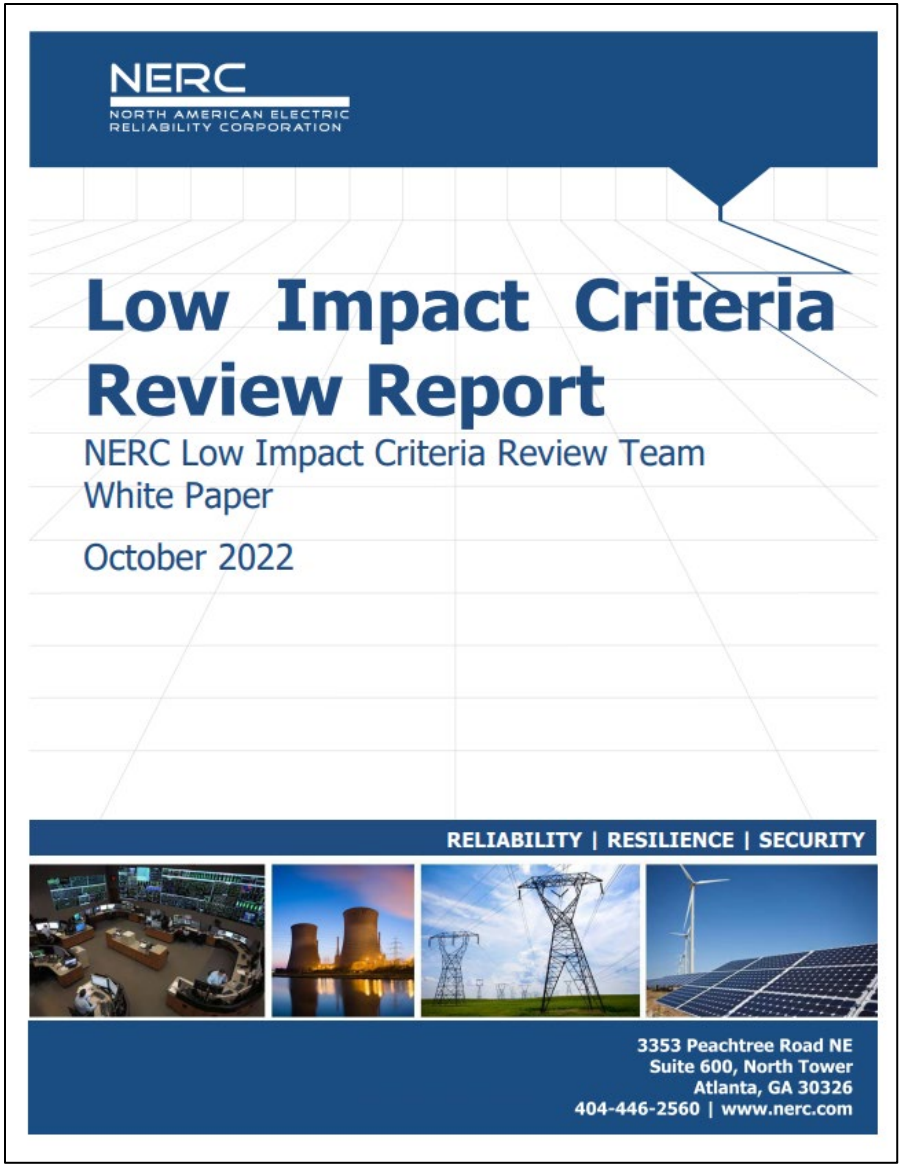
Drafting Team Members

	Name	Entity
Chair	OPEN	OPEN
Vice Chair	Jay Cribb	Southern Company
Members	Monica Jain	Southern California Edison
	Clayton Whitacre	Great River Energy
	Barry Jones	Western Area Power Administration
	Robert Montgomery	Duke Energy
	Peggy McDannald	Associated Electric Cooperative, Inc.
	Josef Chesney	Powder River Energy Corp
	Sean Randles	Leeward Renewable Energy, LLC
	Lemon Williams	Pine Gate Renewables

Agenda

- Background and Overview
- Modifications to CIP-003-9
- Implementation Plan
- Q&A

Background


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Low Impact Criteria Review Report

NERC Low Impact Criteria Review Team White Paper

October 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

LICRT Report Recommendations

- LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems
- LICRT Report
- CIP Standard Revisions
  - 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.
- Project 2023-04 SAR includes the LICRT recommendations

Timeline

July 2023

SAR Revisions

- Consideration of Comments
- SAR accepted by SC

September 2023

Quality Review

- Approved for Oct SC meeting

August 2023

Drafting

- CIP-003-A
- Technical Rationale
- Implementation Plan

Oct-Dec 2023

Initial Posting

- Oct 24 to Dec 7, 2023

CIP-003-9, R2 & Attachment 1

- **Requirement 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 cybersecurity plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.
- **Attachment 1**: Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.
- Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

CIP-003-9 Attachment 1, Section 3

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

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

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

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

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

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

CIP-003-9 Attachment 1, Section 6

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Modifications to CIP-003

- Based on the content of Sections 3 and 6, and the scope of the SAR, the DT decided to merge the two sections
  - Create single section for all electronic access controls
  - Minor impact: Section 6 not implemented until April 1, 2026
  - Minor conforming changes to language: “implement controls” replaces “implement a process” and “implement one or more methods”
- Agreed to maintain existing language of Section 3.1, rather than create a Glossary Term(s) for Low Impact External Routable Connectivity (LERC)
- Updated Attachment 2 with examples of evidence

Requirement Mapping

CIP-003-9 (current)	SAR	CIP-003-A (new)
3.1 (i) - (iii)		Becomes 3.1, “connectivity that provides the ability to communicate” (i) – (iii)
3.1 - **Permit**		Becomes 3.1.1
6.3 - **Detect malicious** (vendor)	SAR	Becomes 3.1.2, and expands to all communications
	SAR	New 3.1.3, **Authenticate users**
	SAR	New 3.1.4, **Protect user authentication info**
6.1 - **Determine** (vendor)		Becomes 3.1.5
6.2 - **Disable** (vendor)		Becomes 3.1.6
3.2 - **Authenticate Dial-up**		Remains 3.2

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

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

3.1 For connectivity that provides the ability to communicate:

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

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

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

3.1.1 Permit only necessary inbound and outbound electronic remote access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic remote access;

3.1.3 Authenticate users when permitting each instance of electronic remote access to networks containing low impact BES Cyber

CIP-003-A (continued)

Systems;

3.1.4 Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems;

3.1.5 Determine vendor electronic remote access, where vendor electronic remote access is permitted; and

3.1.6 Disable vendor electronic remote access, where vendor electronic remote access is permitted.

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

New Electronic Access Controls

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic remote access;

- Anti-malware technologies;
- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
- Automated or manual log reviews;
- Alerting; or
- Other operational, procedural, or technical controls.

New Electronic Access Controls

3.1.3 Authenticate users when permitting each instance of electronic remote access to networks containing low impact BES Cyber Systems;

- Authentication mechanism(s) including but not limited to:
  - Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or
  - Enforcement of Multi-Factor Authentication (MFA).
- Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters; or
- Other operational, procedural, or technical controls.

New Electronic Access Controls

3.1.4 Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems;

- The intent is not to enforce end-to-end protection/encryption.

- Protection mechanism(s) including but not limited to:
- Implementation of an encrypted protocol or service (Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.); or
- Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.
- Other operational, procedural, or technical controls.

Implementation Plan

- Implementation Plan
- Three (3) years from regulatory approval to be compliant with CIP-003-A
- Revise cyber security policy, plan, and procedures.
- Hire and train new staff to implement the new cyber security controls.
- Reconfigure system, network, or security architectures.
- Purchase and procurement of new technology(s).
- Install new technology(s) at all assets containing low impact BES Cyber Systems.
- The effective date of CIP-003-9 is April 1, 2026. CIP-003-A builds upon the implementation of CIP-003-9 for vendor remote access.

Next steps

- Ballot pools formed through November 27, 8:00 p.m.
- Initial ballot for CIP-003-A and implementation plan, November 28 – December 7, 8:00 p.m.
- Supplemental nomination period for DT members until December 7
- CIP-003-10 revisions will eventually be merged with CIP-003-A based on the timing and results of respective ballots. Final ballot of CIP-003-A will likely include CIP-003-10 revisions (acronyms and Section 3.1 revisions).

Questions and Answers