NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-9

October 2022

RELIABILITY | RESILIENCE | SECURITY




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

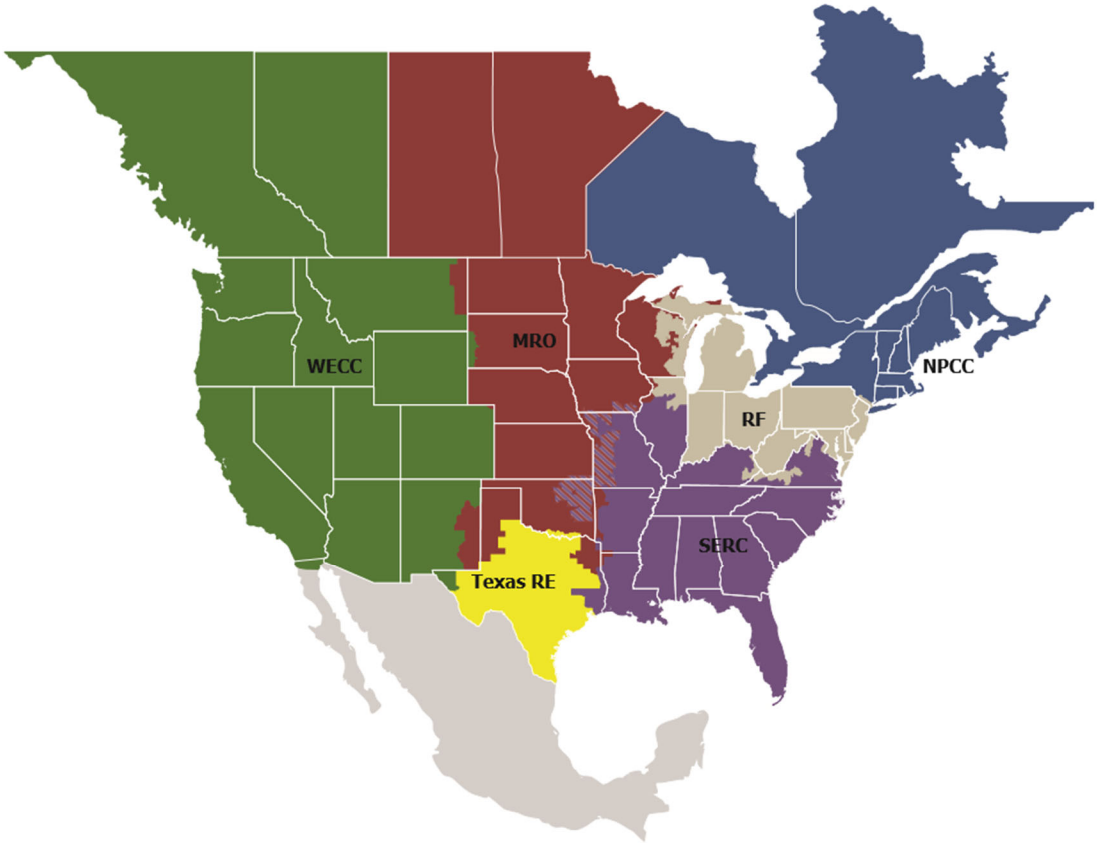
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Technical Rational for Reliability Standard CIP-003-9

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-9. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-9 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2020-03 – Supply Chain Low Impact Revisions Standards Drafting Team (SDT) intent in drafting changes to the requirement.

Background

In its final report[1] accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact Bulk Electric System (BES) Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through Member Representatives Committee (MRC) Policy Input.

After considering policy input, the NERC Board adopted a resolution[2] to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Foreword Regarding Section 3 and Section 6

When developing the standards language for this SAR, the SDT considered many variables and inputs to draft clear, concise, and meaningful requirements. The SDT considered the scope and variety of entity sizes, functions, organizations, systems and configurations, entity business processes, remote access, local electronic access, remote access architectures and technologies, and data path and communications protocols. The SDT discussed systems used for electronic access, remote vs local electronic access, vendor access accounts and privileges, and optimal time frames for establishing, identifying, determining, and disabling or terminating vendor electronic access.

The SDT reviewed industry comments and draft language suggestions, existing standards, and discussed and deliberated the options and their potential impacts and interpretative values to industry. The SDT recognized that some entities may use the same process, system and/or technology (for vendor electronic access) that is used by entity personnel, or cases where entities use separate processes, systems, or technologies to manage vendor electronic access. The SDT also discussed systems and Cyber Assets owned by vendors but authorized for use on entity networks, vs systems and Cyber Assets owned by entities but used by vendors for electronic remote access. Because of the variety, the SDT focused on allowing entities to identify their particular risks related to remote vendor electronic access and define processes and plans to define and implement security controls to address those risks.

[1] Supply Chain Risk Assessment Report (nerc.com)
[2] FINAL_Minutes_BOT_Open_Meeting_February_2020.pdf (nerc.com)

In reviewing the industry comments, the SDT identified, discussed and considered additional terms for clarification, and came to the following conclusions:

1. Electronic remote access: considered remote access as definition and/or remote access vs electronic remote access - as well as onsite vs off-premises remote access. The use of electronic remote access clarifies the remote access using a method (non-physical) which matches existing electronic remote access in other CIP standards.
2. Interactive Remote Access: avoided the existing NERC Glossary of Terms definition in order to prevent applying high and medium impact requirements upon low impact assets and systems.
3. Active: avoided using this term due to potential unintended consequences. The use of "active" may add further requirements upon entities to define, track and document when "active" occurs vs when it does not.
4. Read-only: avoided using this term due to potential unintended consequences. The use of "read-only" may add further requirements upon entities to define and document systems and processes which are read-only from read-write, and where and when read-only access occurs.
5. Vendor: CIP-013 Supplemental Material[3] addresses the term vendor in context with applicable high and medium BES Cyber Systems. The SDT avoided defining the term vendor specifically within the low impact standards to avoid conflicts for entities with high, medium, and low impact systems.

The language developed gives entities the flexibility to define processes to identify and manage vendor electronic remote access for their specific policies, processes, systems, configurations, organizations, operations, and BES Facilities. The language allows entities to define how and where vendor electronic remote access occurs and the ideal methods and timeframes to authorize, establish, and disable vendor electronic remote access.

The SDT agreed to retain Section 3 of CIP-003-9 Requirement R2, Attachment 1 and established Section 6 to specifically address low impact vendor electronic remote access, as well as malicious inbound and outbound data communications which may be sourced from or transmitted to vendors. Based on the SAR, the SDT did not include dial-up from Section 3.2.

The language requires an entity to develop and implement a process or processes for identifying vendor electronic remote access, having a method or methods for disabling vendor electronic remote access, as well as methods to detect known or suspicious vendor inbound and outbound malicious communications.

Entities may choose to define systems, applications and/or configurations used by vendors, accounts and privileges, network data communication paths or physical processes for establishing and disabling vendor electronic remote communications. Section 6 provides the flexibility to meet many types of vendor electronic remote access configurations while managing vendor electronic remote access risks.

Rationale Section 6 of Attachment 1 (Requirement R2)

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In February 2020, the NERC Board approved the initiation of a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine vendor electronic remote access is initiated; and (3) disable vendor electronic remote access when necessary.

As published in the December 2019 NERC Report: Supply Chain Risk Assessment – Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request, of the 87% of section 1600 data request respondents with low impact BES Cyber Systems approximately 66% have external connectivity which often results in the allowance of vendor electronic remote access. As our grid has grown more complex, the use of external parties to support and

[3] CIP-013 Technical Rationale

maintain low impact BES Cyber Systems, equipment and facilities is expected. However, the prevalence of external connectivity across low-impact BES systems could pose a significant impact to the reliability of the grid through the potential of a common supply chain vulnerability. To address this vulnerability, the originating FERC Order[4], and the resulting NERC Board resolution[5], the proposed Attachment 1 Section 6, as it relates to the existing Requirement R2, mandates that applicable entities develop, document, and implement a process to mitigate the risks associated with malicious communications and vendor electronic remote access.

Attachment 1 Section 6 Part 6.1 – Determining vendor electronic remote access

The objective of Attachment 1 Section 6.1 is for entities to determine vendor electronic remote access 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. The obligation in Section 6.1 requires that entities have one or more methods for determining vendor electronic remote access.

Attachment 1 Section 6 Part 6.2 – Disabling vendor electronic remote access

The objective of Attachment 1 Section 6.2 is for entities to have the ability to disable vendor electronic remote access 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. The obligation in Section 6.2 requires that entities have a method to disable vendor electronic remote access, which in turn supports the security objective to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications

The objective of Attachment 1 Section 6.3 is for entities to have the ability to detect known or suspected malicious communications from vendors, such that the entity may respond to and remediate any resulting adverse impacts.

This sub section is scoped to focus only on vendors' communications per the NERC Board resolution and the supply chain report. The obligation in Section 6.3 requires that entities must establish a method(s) to detect known or suspected malicious communications from vendors and the systems used by vendors to communicate with assets containing low impact BES Cyber Systems.

Current obligations in CIP-003-8 Requirement R2 that govern direct electronic communications with low impact BES Cyber Systems are not as robust as those in CIP-005-6 that govern high impact medium impact BES Cyber Systems. Security controls such as use of Intermediate Systems and multi-factor authentication provide additional security protection from malicious communication and overall access controls for high and medium impact BES Cyber Systems. In addition to Intermediate Systems and multi-factor authentication, high and medium impact BES Cyber Systems at Control Centers have requirements to detect malicious communications at the Electronic Access Points of those systems. These security measures are not required at low impact BES Cyber Systems.

In keeping with the NERC stated risk-based model, there may be a scenario where a vendor directly communicates with a low impact BES Cyber System. In the event that this connection may be compromised, the inclusion of security requirements to detect malicious communications under CIP-003-9 Attachment 1 Section 6 would provide entities visibility and opportunity in detecting and mitigating risks posed by vendor communications.

[4] Order No. 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016).

[5] Resolution-Supply Chain Recommendations - Board Approved - February 6, 2020 (LINK)