NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Security Management Controls

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

August 2021

RELIABILITY | RESILIENCE | SECURITY




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

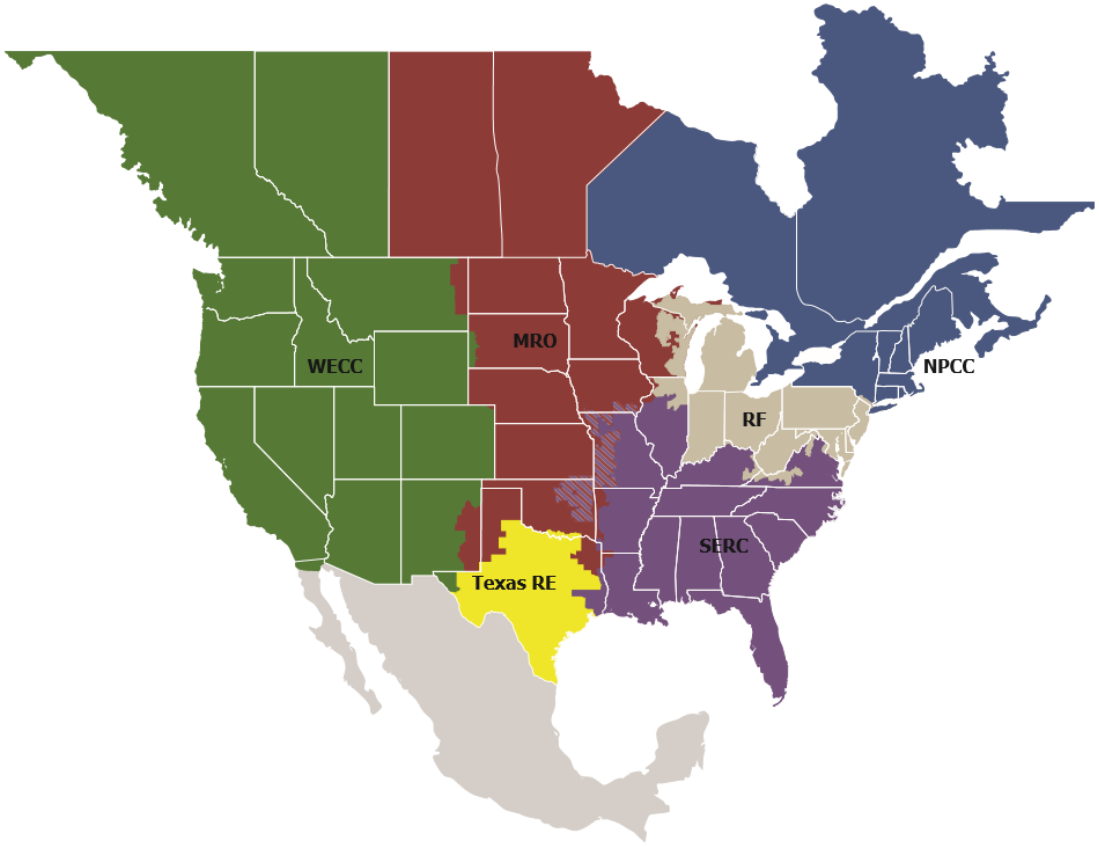
Table of Contents

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-X

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-X. 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-X 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 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 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 MRC Policy Input.

After considering policy input, the NERC Board adopted a resolution 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.

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 when active vendor remote access sessions are initiated; and (3) disable active vendor 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 67% have external connectivity which often results in the allowance of 3rd party access. As our grid has grown more complex, the use of third parties to support and maintain low impact BES Cyber Systems, equipment and facilities is expected; However, the prevalence of external connectivity and 3rd party access, herein referred to as vendor[1] remote access, 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

[1] Similar to CIP-013, the term *vendor(s),* as used in the standard, is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

vulnerability, the originating FERC Order[2], and the resulting NERC Board resolution[3] the proposed Attachment 1 Section 6, as it relates to the existing Requirement 2, mandates that applicable entities develop, document, and implement a process to mitigate the risks associated with malicious communications and vendor remote access. This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems.

Attachment 1 Section 6 Part 6.1 – Determining Vendor Remote Access

The objective of Attachment 1 Section 6.1 is for entities to have visibility of vendor remote access sessions (including interactive remote access and system-to-system) that are taking place on their low impact BES Cyber Systems. Such visibility increases an entities ability to rapidly detect, respond and resolve issues that may originate with or be tied to a particular vendor's remote access session. The obligation in Section 6.1 requires that entities have a method to determine active vendor remote access sessions, R2 requires that said method be documented and implemented.

In support of Attachment 1 Section 6.3, and in line with FERC Order No. 829 (p.49), increased vendor remote access visibility may give Responsible Entities the ability to rapidly disable remote access sessions in the event of a system breach.

Attachment 1 Section 6 Part 6.2 – Detecting known or suspected malicious communications for both inbound and outbound communications

The objective of Attachment 1 Section 6.2 is for entities to have the ability to detect known or suspected malicious communications such that the entity may respond to and remediate resulting impacts. The obligation in Section 6.2 requires that entities which allow vendor remote access (including interactive remote access) must establish a process/procedure to detect malicious communications from vendors and the systems used by vendors to access low impact BES Cyber Systems. R2 requires that these methods be documented and implemented.

Attachment 1 Section 6 Part 6.3 – Disabling vendor remote access

The objective of Attachment 1 Section 6.3 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52). Per FERC Order 829 (p.49), the inability of a responsible entity to rapidly terminate a connection may allow malicious or otherwise inappropriate communication to propagate, contributing to a degradation of a BES Cyber Asset's function. Enhanced visibility into remote communications and the ability to rapidly terminate a remote communication could mitigate such a vulnerability. The obligation in Section 6.3 requires that entities have a method to disable active vendor remote access sessions, R2 requires that said method(s) be documented and implemented.

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

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