AMPERE

New Low Impact NERC CIP-003-9 Regulations: Vendor Supply Chain Security

Webinar 6 April 2023

Introduction

Patrick Miller

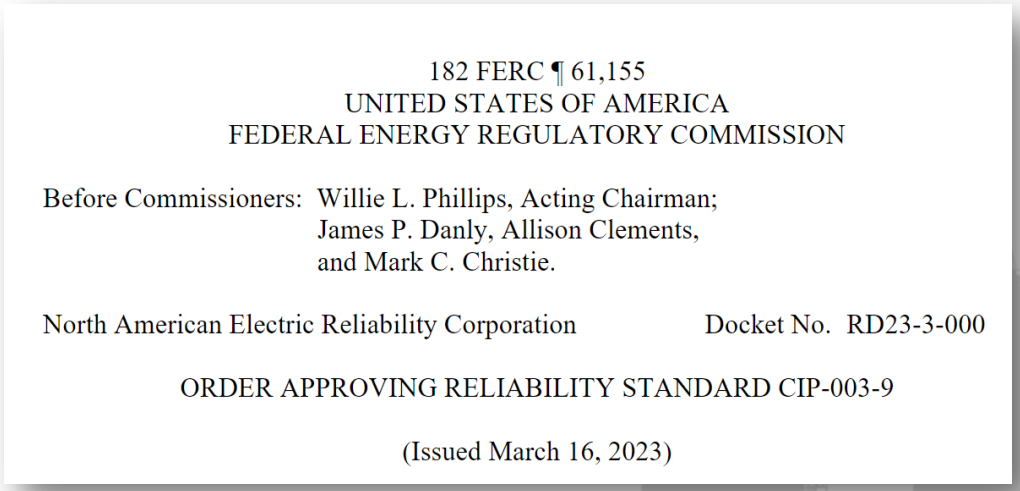
Ron Fabela

Jason Smith

Carter Manucy

What Happened?

FERC Order approving update to CIP-003-9 On March 16th, 2023



182 FERC ¶ 61,155
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Willie L. Phillips, Acting Chairman;
James P. Danly, Allison Clements,
and Mark C. Christie.

North American Electric Reliability Corporation Docket No. RD23-3-000

ORDER APPROVING RELIABILITY STANDARD CIP-003-9

(Issued March 16, 2023)

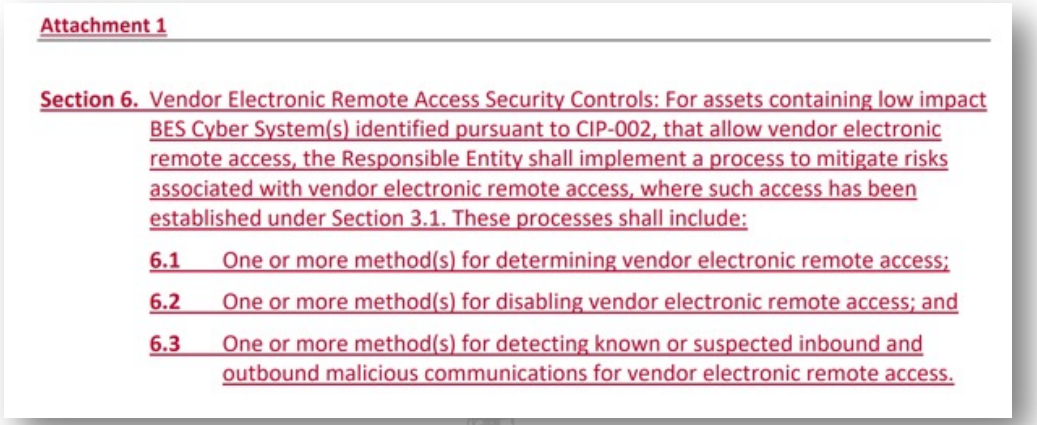
*"adding new requirements focused on **supply chain risk management** for low impact bulk electric system (BES) Cyber Systems"*

CIP 003-9 Updated
https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-003-9.pdf

Overview of Changes

Additions:
Section 6. Vender Electronic Remote Access Security Controls

Subtractions:
Entire *"Guidelines and Technical Basis"* and Reference Models



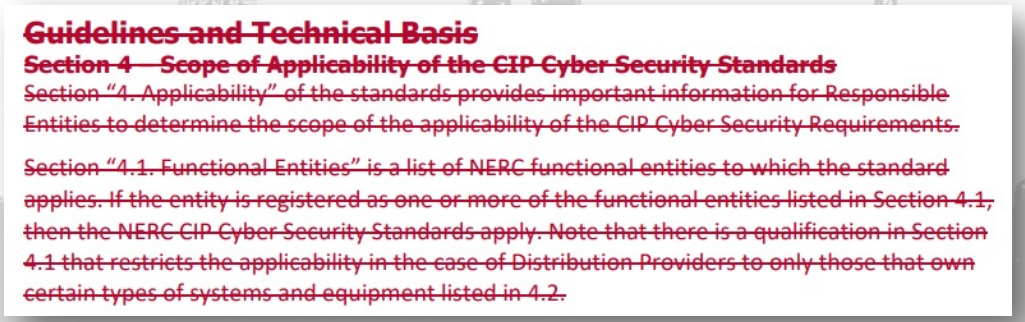
Attachment 1

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.



~~**Guidelines and Technical Basis**~~

~~**Section 4 – Scope of Applicability of the CIP Cyber Security Standards**~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

Why This Update?

- Section 1600 Data Request
- Risk Assessment Report
- Standards Authorization Request
- CIP-003-09

Why This Update?

Supply Chain Risk Assessment Report

https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply%20Chain%20Risk%20Assesment%20Report.pdf

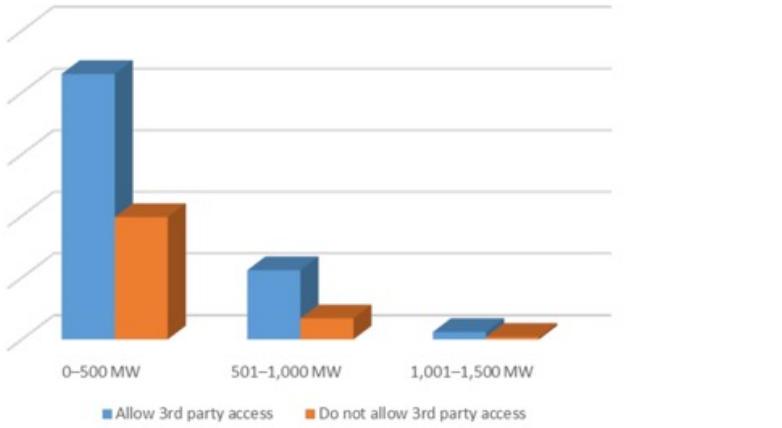


Figure 2.9: Generation Resources for Entities with only Low Impact BES Cyber Systems

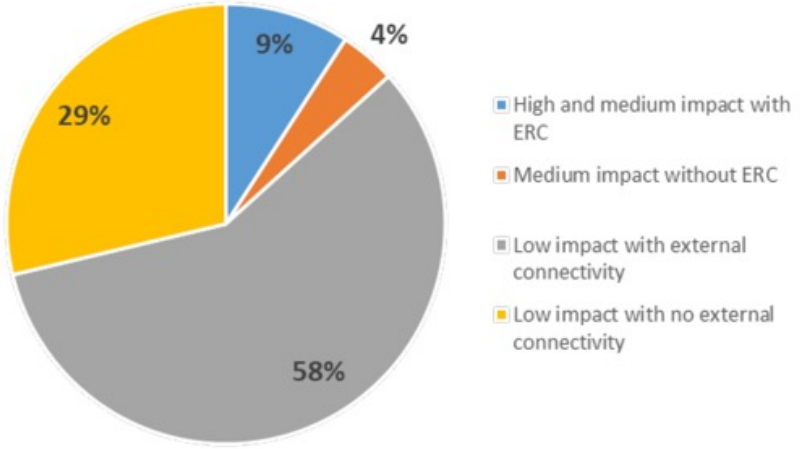


Figure 2.1: All Locations Containing BES Cyber Systems

"[regarding CIP low generation assets] A significant percentage of these locations allow third-party access"

Why This Update?

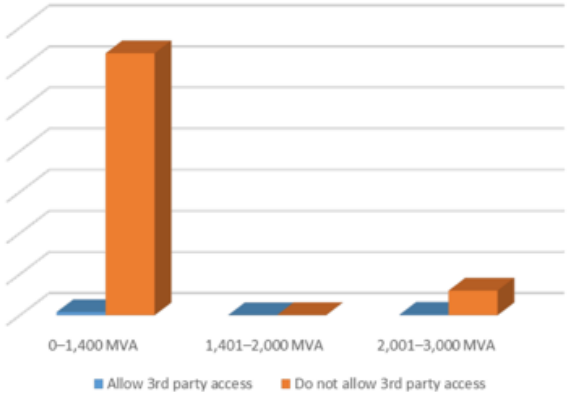


Figure 2.6: Transmission Stations and Substations for Entities with High, Medium, and Low Impact BES Cyber Systems

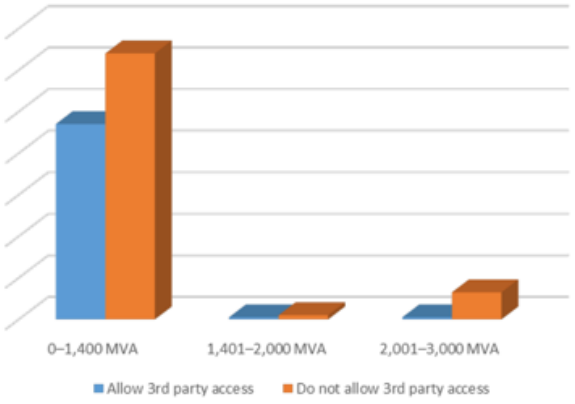


Figure 2.7: Transmission Stations and Substations for Entities with only Low Impact BES Cyber Systems

Delta between high, medium and low impact entities vs. those with just low impact

Why This Update?

- “While these locations represent a small percentage of all transmission stations and substation locations, the combined effect of a coordinated cyberattack on multiple locations could impact BES reliability beyond the local area.”

- Coordinated cyber attack is a theme that's being used to drive home a number of changes in low impact

Curiosities and Conversation

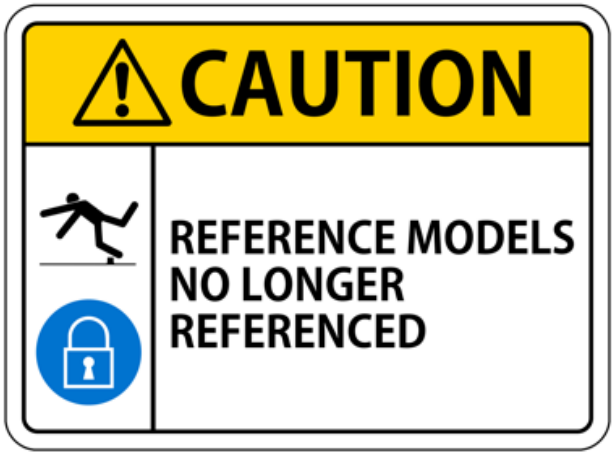
- FERC Order, Docket RD23-3-000:
  - "…we determine that proposed Reliability Standard CIP-003-9 improves upon the currently effective Reliability Standard CIP-003-8 by adding new requirements focused on supply chain risk management for low impact bulk electric system (BES) Cyber Systems."

- This has nothing to do with the Supply Chain Risk Management standard, CIP-013 however it is important to have a consistent approach towards vendors throughout the standards
- It is much closer to CIP-005.R3

Curiosities and Conversation

If CIP Low Impact Sites Do Not Have an “ESP” – What Does “Remote” Mean for 003-9?

Where Did Our Reference Models Go?



Curiosities and Conversation

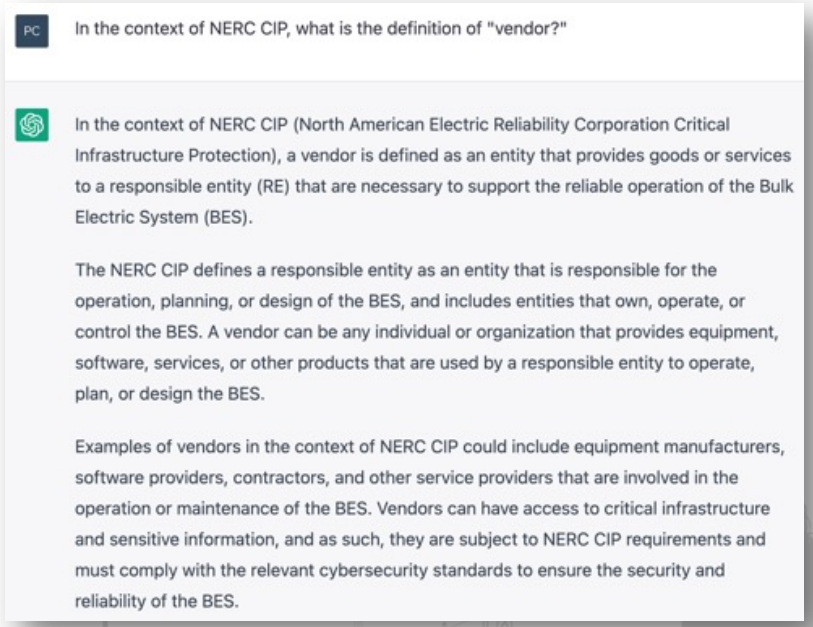
- Multiple bites at the apple – 4 drafts
- 6.3 in particular…
- Previous draft was:
  - 6.3. One or more method(s) for detecting known or suspected inbound and outbound malicious communications.
- Now it reads:
  - 6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Curiosities and Conversation

- The drafting team was highly aware of the difference between "remote access" and "remote monitoring”
- Probable challenges with auditors will be around what "remote access" means
  - “remote access” vs “remote control”
- To be safe protect ALL communications (monitoring) in the event something bad happens
- NERC wants ALL of it monitored & controlled

Curiosities and Conversation

What's a Vendor?



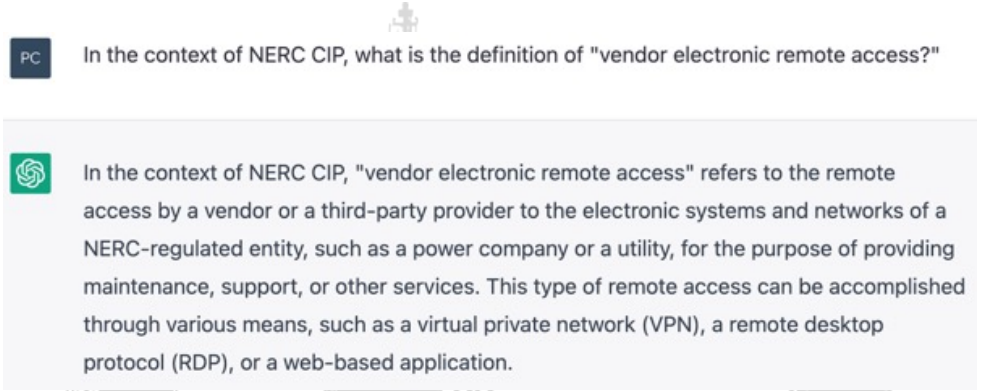
PC In the context of NERC CIP, what is the definition of "vendor?"

In the context of NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection), a vendor is defined as an entity that provides goods or services to a responsible entity (RE) that are necessary to support the reliable operation of the Bulk Electric System (BES).

The NERC CIP defines a responsible entity as an entity that is responsible for the operation, planning, or design of the BES, and includes entities that own, operate, or control the BES. A vendor can be any individual or organization that provides equipment, software, services, or other products that are used by a responsible entity to operate, plan, or design the BES.

Examples of vendors in the context of NERC CIP could include equipment manufacturers, software providers, contractors, and other service providers that are involved in the operation or maintenance of the BES. Vendors can have access to critical infrastructure and sensitive information, and as such, they are subject to NERC CIP requirements and must comply with the relevant cybersecurity standards to ensure the security and reliability of the BES.

What's Vendor Electronic Remote Access?



PC In the context of NERC CIP, what is the definition of "vendor electronic remote access?"

In the context of NERC CIP, "vendor electronic remote access" refers to the remote access by a vendor or a third-party provider to the electronic systems and networks of a NERC-regulated entity, such as a power company or a utility, for the purpose of providing maintenance, support, or other services. This type of remote access can be accomplished through various means, such as a virtual private network (VPN), a remote desktop protocol (RDP), or a web-based application.

Implementation Plan

CIP	CIP-003-9	Cyber Security — Security Management Controls	4/1/2026

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-9 as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.6 on or before the effective date of CIP-003-9.

Responsible Entities shall initially comply with all other periodic requirements in CIP-003-9 within the periodic timeframes of their last performance under CIP-003-8.

https://www.nerc.com/pa/Stand/202003_Supply_Chain_Low_Impact_Revisions_DL/2020-03_CIP-003-9_Implementation_Plan_clean_10262022.pdf

What Should You Do?

- Determine if you even want to allow remote electronic access for vendors to low impact assets – but think future, not now
  - This could be a great “motivator” for modernization projects
  - Ensure that the section 6 requirements are being considered
  - Easier to do assessments on current architecture but future changes may slip through the cracks
- What solution are you using for H/M CIP-005.R3 – and will that work for this? If not, decide which types of access you will allow and if this will require:
  - A change to architecture
  - New technologies
  - New processes
- Architecture assessments are crucial
  - Know for certain how data flows in and out of your environments

What Should You Do?

- Identify all individuals who play a role in the relevant operations
- They will know which vendors they work with
- CIP-012 RTA/RTM teams may also be useful
- Identify all vendors
  - Do they have some form of access?
  - Systems level, network level or application level?
- Don't just talk to IT/OT and assume you've covered your bases

What Should You Do?

- Work with your vendors early
  - What do they think about the standard?
  - What are they planning on doing?
- Put your own equipment in place
  - Can't always trust the vendor to do it in a compliant manner
  - You are the RE, not them
- Another option is to take control over the equipment they have installed and check their work

What Should You Do?

- Begin gathering the evidence and prepare documentation
- Start with the violation language and work backwards
  - Failed to document its cyber security process for vendor electronic remote access security controls
  - Failed to document and implement its cyber security process for vendor electronic remote access security controls
- Don’t get tripped up on the document side especially if you have little to no remote access to begin with
- Don’t wait to begin work; this will take longer than you think

Questions?

Patrick C Miller

Email: pmiller@amperesec.com

LinkedIn: https://www.linkedin.com/in/millerpatrickc/

Twitter: @patrickcmiller

Mastodon: @patrickcmiller@infosec.exchange

Jason Smith

Email: jsmith@amperesec.com

LinkedIn: https://www.linkedin.com/in/jason-smith-02a33072/

Twitter: @skeetwick

Ron Fabela

Email: rfabela@amperesec.com

LinkedIn: https://www.linkedin.com/in/ronniefabela/

Twitter: @ron_fab

Carter Manucy

Email: carter.manucy@nreca.coop

LinkedIn: https://www.linkedin.com/in/cmanucy/

Twitter: @cmanucy