Compliance and Advisory Services
RELIABILITY MATTERS

CIP Low Impact – 2024

Over time, FERC has added more requirements for Low Impact entities regarding Cyber Protection Infrastructure (CIP) controls to protect the integrity of the Bulk Electric System (BES).

As anyone with a cell phone, tablet, or computer knows, bad actors with malicious intent are continuously searching for potential vulnerabilities in access controls to launch attacks.

In their order regarding **CIP-003 version 9**, NERC highlighted the heightened risk if multiple Low Impact assets are compromised at the same time through remote access, or if a Medium or High Impact asset is accessed through a Low Impact asset. With this in mind, a targeted attack on all software users at a specific plant poses a persistent and genuine threat. If a third-party vendor supplying or servicing the software is infiltrated, it can directly harm the BES.

This ongoing risk is because the majority of combined-cycle control systems in the U.S. are sourced from a few gas-turbine vendors and one or two control-system Original Equipment Manufacturers (OEMs).

To address this risk, FERC and the electric industry have **expanded CIP requirements applicable to Low Impact registered entities**. FERC approved CIP-003 version 9 on March 16, 2023, with **enforcement starting on April 1, 2026**. This version addresses **supply chain risk management of Low Impact BES Cyber Systems**.

The order mandates responsible entities to include the topic of **'vendor electronic remote access security controls'** in their cyber security policies. It also requires these responsible entities to have **methods for determining and disabling vendor electronic remote access** for assets containing Low Impact BES Cyber Systems.

Supply chain controls have been in place for Medium and High Impact entities since 2017, offering valuable insights for developing and implementing plans for CIP-003-9 enforcement.

Specific sections of CIP-003-9 applicable to Low Impact assets include:

R1.2.6. Vendor electronic remote access security controls

Attachment 2, 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.

hsi.com/industrial-skills

800.447.3177
industrial-skills@hsi.com