TEXAS RE

2025 CMEP IP

Devin Ferris
Manager, CIP Compliance Monitoring

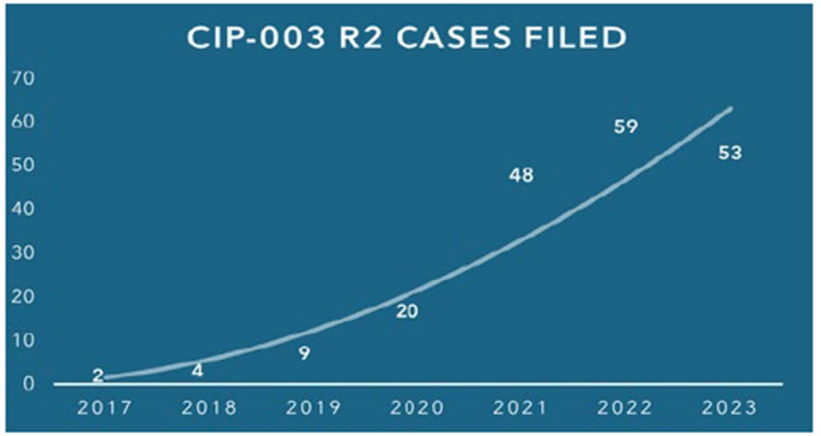
January 10, 2025

2025 CMEP IP

2024	2025
Remote Connectivity	Remote Connectivity
Supply Chain	Supply Chain
Physical Security	Physical Security
Incident Response	Incident Response
Stability Studies	Transmission Planning and Modeling
Inverter-Based Resources	Inverter-Based Resources
Facility Ratings	Facility Ratings
Extreme Weather Response	Extreme Weather Response

2024 CIP Themes and Lessons Learned Report

Remote Connectivity



The protection of critical infrastructure remains a major focus for the 2025 risk areas. With remote connectivity and the use of remote workers continuing, it is vitally important that facility staff understand the changes taking place with their technology and have a better understanding of how to protect it. The ERO Enterprise has seen poor security practices (a) remotely unlocking doors for unauthorized individuals; (b) neglecting to secure doors and manage keys; and (c) generally failing to identify a need to create or apply security plans to new sites or sites transitioning from medium/high to low impact.[5] Root causes in these cases often point to ineffective training and lack of direction or guidance, which can result in staff treating low impact sites as functionally out of scope for NERC CIP purposes, which in turn can increase the frequency of less-than-desirable security decisions.

As security needs evolve, the ERO Enterprise and industry must remain vigilant, identify any gaps, and mitigate, as necessary. There is a noticeable trend as it relates to low impact BES Cyber Systems. As noted in the 2024 CIP Themes and Lessons Learned Report, a compromise of such assets could create localized issues, and an individual low impact asset could (a) serve as a channel to attack other assets or (b) be used to conduct reconnaissance. And the potential risk to the BES multiplies in scenarios where several low impact assets are compromised in a coordinated attack.[6]

Regardless of the sophistication of a security system across all types of BES facilities, there is potential for human error. Compliance monitoring should seek to understand how entities manage the risk of remote connectivity and the complexity of the tasks the individuals perform.

CIP-003-9 Effective Date

- Vendor Electronic Remote Access Security Controls

April 01, 2026

Vendor Electronic Remote Access Security Controls

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.

TEXAS RE
Ensuring electric reliability for Texans