



CIP-003-9 SUPPORT

Strengthening Security Management Controls for Low Impact BES Cyber Systems

NAES Asset Solutions provides technical Operational Technology (OT) support to help owners evaluate the security controls, processes, and documentation supporting NERC CIP-003-9 requirements for low impact BES Cyber Systems.

The engagement provides facility leadership with an independent technical view of current OT security-control readiness, identified gaps, and remediation priorities. Asset Solutions supports the technical OT environment and does not replace the facility's NERC CIP Compliance Manager or NAES NERC Services.

WHY CIP-003-9 MATTERS

CIP-003-9 Security Management Controls became effective April 1, 2026. The standard adds requirements for low impact BES Cyber Systems related to malicious communications and vendor remote access.

The updated requirements include policies to:

- Detect known or suspected malicious communications for both inbound and outbound communications
- Determine when active vendor remote access sessions are initiated
- Disable active vendor remote access when necessary

For facility owners, the challenge is not only having a policy. Technical controls, OT configurations, processes, and supporting documentation must align with the facility's actual operating environment.

HOW NAES SUPPORTS CIP-003-9 READINESS

NAES Asset Solutions can perform a focused OT compliance check and technical review to help identify gaps between required security controls and the way the facility's OT environment is configured and operated. The engagement may include:

OT Compliance Check - Review relevant OT security controls, processes, and supporting documentation to provide an independent view of current technical compliance posture.

Communications Monitoring Readiness Review - Evaluate the technical environment supporting visibility into inbound and outbound communications for low impact BES Cyber Systems.

Vendor Remote Access Review - Review how vendor remote access is initiated, monitored, controlled, and disabled within the OT environment.

Vulnerability & Configuration Review - Evaluate system configurations, software, network architecture, and procedures for technical weaknesses that may affect security or control-system reliability.

Backup & Recovery Review - Assess backup and recovery design for critical control-system assets and identify gaps in restoration readiness.

Focused Cybersecurity Training - Provide OT-specific cybersecurity training incorporating NERC CIP principles where applicable.

Scope note: Asset Solutions provides technical OT assessment and support. It does not serve as the facility's NERC CIP Compliance Manager and does not author or formally validate official NERC CIP procedures. This work supports, not replaces, NAES NERC Services.

WHAT YOU RECEIVE

A CIP-003-9 Support engagement can provide:

- A documented independent review of the OT technical controls included in the agreed scope
- Identification of security-control, configuration, process, and documentation gaps
- Observations related to communications monitoring and vendor remote access controls
- Prioritized technical recommendations for identified gaps
- Identification of OT vulnerabilities or single points of failure relevant to the review
- A remediation roadmap that can be coordinated with the facility's compliance leadership or NAES NERC Services

The output is intended to help facility leadership understand the technical condition of the OT environment and where focused action may be required.

WHERE THIS FITS

CIP-003-9 Readiness - Evaluate OT technical controls supporting the current low impact BES Cyber System requirements.

Audit Preparation - Provide an independent technical review of OT controls, configurations, and supporting evidence before a regulatory review or audit.

Vendor Remote Access Changes - Review technical controls when new vendors, remote-access methods, or support processes are introduced.

DCS or OT Network Changes - Reassess applicable security controls following major platform, network, architecture, or control-system changes.

Following a Cyber or Controls Event - Review the OT environment after an incident, near miss, or unverified device interaction.

Periodic Compliance Checks - Use focused technical reviews to provide leadership with an updated view of OT security-control posture.

CIP-003-9 Support can be delivered as a focused Asset Solutions engagement and coordinated with NAES NERC Services when broader compliance-program support is required.

VALUE TO OWNERS AND OPERATORS

- Clearer visibility into the technical OT controls supporting CIP-003-9 requirements
- Earlier identification of gaps involving communications monitoring and vendor remote access
- Better alignment between OT technical practices and compliance requirements
- Prioritized technical remediation actions
- Improved coordination between plant OT personnel and compliance leadership
- Independent technical insight without transferring formal compliance ownership

Engage NAES Asset Solutions for an independent technical review of the OT controls supporting CIP-003-9 readiness and low impact BES Cyber System security management.

