

CIP-003-9 Is Not Just a Compliance Update. It Is a Visibility Problem.



Many power producers view CIP-003-9 primarily as a compliance deadline. That perspective is too limited.

In practice, CIP-003-9 compels plants to assess whether they truly understand and can control their OT environment. The challenge lies not in unclear language, but in the technical discipline required where many sites still depend on assumptions, legacy decisions, and limited visibility.

CIP-003-9 establishes security management controls intended to protect BES Cyber Systems against compromise that could lead to misoperation or instability within the Bulk Electric System. It applies to registered Generator Owners and registered Generator Operators, and for entities other than certain Distribution Providers, it applies broadly to BES Facilities. Under Requirement 1, entities must maintain documented cyber security policies. Under Requirement 2, entities with applicable low impact BES Cyber Systems must implement documented cyber security plan(s) that include the sections in Attachment 1.

While this outlines the regulatory structure, the operational question is straightforward: Do you know what is connected, routable, remotely accessible, active, and capable of affecting your plant?

The Core Issue Is OT Visibility, Not Policy.

When defining OT for plant teams, we focus on the equipment and infrastructure not typically managed by corporate IT, but essential for plant operations. This includes control platforms, firewalls, switches, HMIs, DAHS, servers, gateways, historians, support workstations, and the communications paths that maintain plant operations. OT risk reduction starts with visibility across these components.

This is where many plants are weaker than they think.

Over time, systems accumulate: vendor servers remain after startup, obsolete OPC connections persist, and telemetry paths survive multiple upgrades and staffing changes. Temporary remote support methods often become permanent without proper review. As a result, plants may believe they understand their control boundaries, while the actual architecture has changed. CIP-003-9 is designed to expose these discrepancies.

While the standard does not require an inventory or discrete identification of low impact BES Cyber Systems under Requirement 2, that should not be interpreted as permission to remain vague. Without clear knowledge of what is present and how it communicates, it is difficult to demonstrate that plans are technically sound, implemented, and effective.

Vendor Remote Access Is Where the Standard Gets Real

Attachment 1, Section 6 is where CIP-003-9 becomes immediately practical for many plants.

For assets containing low impact BES Cyber Systems that allow vendor electronic remote access, the standard requires the Responsible Entity to implement a process that mitigates the associated risk. That process must include one or more methods for determining vendor electronic remote access, one or more methods for disabling it, and one or more methods for detecting known or suspected inbound and outbound malicious communications associated with that access.

This requirement is significant because many sites assume remote access is controlled simply by knowing the primary path. That is insufficient.

Plants must be able to identify where vendor electronic remote access exists, how it is established, when it is active, how it can be disabled, and how suspicious traffic is detected. If these questions

cannot be answered clearly, the risk is already present in the architecture. The remaining published RSAWs are still useful mainly as an indicator of how auditors are likely to think, but current compliance monitoring is evidence-based. Auditors will verify that the required processes and controls are in place and operating as intended rather than relying on a specific worksheet or form. This is why we keep coming back to visibility. You cannot disable what you have not identified. You cannot detect malicious communications on a path you do not know exists.

Electronic Access Controls Must Be Defensible, Not Assumed

Attachment 1, Section 3 requires electronic access controls that permit only necessary inbound and outbound electronic access for qualifying routable communications crossing the asset boundary. It also requires authentication for dial-up connectivity, where applicable and where the Cyber Asset is capable of it.

Too often, plants reduce that requirement to a simple statement: “We have a firewall.”

That is not the standard. The standard is about controlled communications. The firewall is only relevant if it has been configured, maintained, and aligned with the real architecture in a way that supports the security objective.

In practice, that means the entity should be prepared to explain routable communications crossing the boundary, justify why those communications are necessary, identify the devices enforcing control, and show that the configuration supports the intended segmentation. NERC expects entities to be able to defend the architecture at a technical level, not just describe it at a policy level.

CIP-003-9 Also Reaches the Tools That Move In and Out of the Plant

Another reason we view CIP-003-9 as a field standard rather than a paperwork standard is its treatment of transient cyber assets and removable media.

Attachment 1, Section 5 requires one or more plans to mitigate the introduction of malicious code into low impact BES Cyber Systems through transient cyber assets or removable media. That includes plant-managed transient cyber assets, third-party transient cyber assets, and removable media. The standard requires review and mitigation steps before connection, and for removable media it requires both a method to detect malicious code using a separate Cyber Asset and a method to mitigate any detected threat before connection.

This Focus Is Appropriate for Real Operating Environments.

Plants do not exist in sterile conditions. Vendors arrive with laptops, contractors bring tools, and files move during troubleshooting and maintenance. Under time pressure, people make practical decisions. CIP-003-9 is telling the industry that these practical realities still require disciplined controls.

Incident Response at Low Impact Sites Is Still an Operational Requirement

Plants should pay close attention to Attachment 1, Section 4. CIP-003-9 requires one or more Cyber Security Incident response plans that address identification, classification, response, reportability, E-ISAC notification where required, roles and responsibilities, incident handling, periodic testing, and updates following testing or an actual Reportable Cyber Security Incident. The plan must be tested at least once every 36 calendar months, and updates must be made within 180 calendar days if needed after a test or actual Reportable Cyber Security Incident.

Low impact does not equate to low consequence; it indicates a different compliance structure.

From an operating standpoint, a plant still needs to know who acts, who documents, who classifies, who escalates, and who decides whether the event is reportable.

The Implementation Plan Is More Important Than Many Teams Realize

The official NERC Implementation Plan is worth reading because it clarifies how CIP-003-9 takes effect and how periodic requirements transition from CIP-003-8.

The plan states that CIP-003-9 retires CIP-003-8 immediately prior to the new standard becoming effective in the applicable jurisdiction. It also states that, where approval by an applicable governmental authority is required, CIP-003-9 becomes effective on the first day of the first calendar quarter that is 36 months after the effective date of the approving order. The plan further specifies that entities must initially comply with Requirement 1, Part 1.2.6 on or before the effective date of CIP-003-9, while all other periodic requirements remain tied to the periodic timeframes of the entity's last performance under CIP-003-8.

In the United States, that enforcement date was April 1, 2026.

That distinction matters because entities should not view CIP-003-9 as a future documentation exercise. The transition logic is already established. Entities should be validating OT boundaries, addressing access assumptions, reviewing remote connectivity, and aligning evidence to auditor expectations now.

Evidence Will Matter More Than a Worksheet

Current NERC compliance monitoring is evidence-based. Registered entities should expect auditors to evaluate whether required processes and controls are documented, implemented, and operating as intended, and whether the supporting evidence is sufficient and appropriate.

The remaining published RSAWs can still be useful as a readiness aid because they show how auditors are likely to think about the requirement structure, applicable plan sections, and evidence organization. But they should not be treated as the primary compliance artifact.

Our Advice: Start With Architecture, Not Paperwork

CIP-003-9 will certainly drive policy updates, plan revisions, and evidence preparation. But plants that begin there are starting at the wrong end of the problem.

We would start with the architecture.

Identify assets containing low impact BES Cyber Systems. Review routable communications entering and leaving those assets. Determine where vendor remote access exists, how it is authorized, and how it is disabled. Confirm which devices enforce electronic access control. Review practices for transient cyber assets, removable media controls, and incident response testing. Then align documentation to reflect that reality. That sequence produces a more defensible result.

Ultimately, CIP-003-9 is not only concerned with policy language, but with whether the plant has sufficient technical control over its low impact environment to explain, implement, and sustain those policies.

And that is where many sites still have work to do.

Readers who want to review the source documents directly can use the official NERC materials for the [CIP-003-9 standard](#), the [Implementation Plan](#), and the [Reliability Standard Audit Worksheet](#).