

Xona + NERC CIP 003-9

(Effective April 1, 2026)

Powered by



Executive Summary

On **April 1, 2026**, NERC CIP 003.9 becomes enforceable and requires covered entities to implement **Vendor Electronic Remote Access Security Controls** (Section 6). The Xona platform is purpose built for critical infrastructure and has been **third party tested** with mappings to key NERC standards—including **CIP 003.9, CIP 005.5, CIP 007.6, CIP 011.2, and CIP 013.1**—enabling operators to meet the mandate and produce audit-ready evidence with minimal operational friction.

Xona replaces VPNs, jump servers, and other legacy tools with **disconnected access (protocol isolation), MFA, least privilege user to asset controls, and full fidelity session logging/recording**—all delivered through a **zero footprint browser** and managed centrally across fleets and sites.

Xona provides the architecture, controls, and artifacts you need to implement CIP-003-9 Section 6 and demonstrate conformance—while materially reducing OT risk and operational overhead.

What Changes Under CIP-003-9 and How Xona Aligns

Scope highlight – Section 6: documented pre-authorization, monitored vendor access, auditable logs/records, the ability to immediately disable vendor access (including ports/protocols), and processes/technologies to detect malicious communications.

Key CIP Standard Dependencies

CIP-005-5 (Interactive Remote Access)

Xona's Critical System Gateway (CSG) functions as an intermediate system, brokering and isolating sessions, enforcing encryption and MFA.

CIP-011-2 (Information Protection)

Pixel-streaming via TLS safeguards BES Cyber System Information from being exposed to endpoints.

CIP-007-6 (System Security Management)

Detailed event logging for successful/failed logons and session times; configurable retention to ≥ 90 days.

CIP-013-1 (Supply Chain)

Signed/verified updates and documented processes support secure software integrity.

Architecturally, Xona prevents any network connectivity from the user endpoint to the OT asset through **protocol isolation**: OT protocols (RDP, SSH, VNC, HTTPS, etc.) terminate on the trusted side of the CSG and are transformed into an **encrypted, interactive pixel stream over 443** to the user's browser. This breaks lateral-movement paths and keeps OT protocols off untrusted networks.

Control-by-Control Mapping – CIP-003-9 Section 6

6.1 Pre-Authentication; Oversight; Evidence

Xona addresses each CIP-003-9 Section 6 requirement through specific platform capabilities:

Requirement	Xona Capability / Implementation
6.1.1 Steps to pre-authorize access	Zero-trust policy with identity-based RBAC/TBAC assigns specific users to specific assets and time windows; optional moderation adds human-in-the-loop approvals.
6.1.2 Alerts generated by vendor log-on	Moderated Access notifies approvers on vendor arrival; integration points forward events to SIEMs.
6.1.3 Session monitoring	Real-time shadow/monitor roles (Administrator/Monitor) for live oversight and supervisor intervention.
6.1.4 Security information management logging/alerts	Export activity/connection history via Splunk, RSyslog, Generic HTTP.
6.1.5 Time-of-need session initiation	Time/date controls (specific time or ranges) to enforce "need-to-access" windows.
6.1.6 Session recording	Full-fidelity video capture for RDP/SSH/VNC with metadata for e-discovery and non-repudiation.
6.1.7 System logs	Comprehensive system and user connection audit trails with export to SIEM.
6.1.8 Other operational/procedural/technical controls	Zero-trust enforcement, protocol isolation, and brokered input streams (no endpoint-to-asset connectivity).

6.2 How to Disable Vendor Electronic Remote Access

Control	Description
6.2.1 Disable vendor accounts	Lockbox can globally disable CSG access; individual users can be revoked instantly.
6.2.2 Disable ports/services/permissions	Immediate Kill button terminates sessions; Lockbox disables ports; granular policy removes permissions as needed.
6.2.3 Disable communications protocols	Edit Connection allows protocol-level disablement (e.g., RDP/SSH).
6.2.4 Remove physical connectivity	Lockbox can physically disable untrusted/trusted Ethernet ports on the CSG.
6.2.5 Administrative control documentation	Lockbox/disable procedures are documented and demonstrable.
6.2.6 Other controls	Additional zero-trust guardrails and policy controls as compensating measures.

6.3 Detection of Malicious Communications

Control	Description
6.3.1 Anti-malware	Xona's pixel-streaming prevents code flow from the endpoint into the OT protocols; moderated file transfer can enforce malware scans and approvals before any ingress.
6.3.2 IDS/IPS	The CSG, as an isolation/broker layer, does not require inline IDS/IPS; entities may still monitor north-south traffic with existing controls.
6.3.3 Automated/manual log reviews	Export data + video logs for automated review or manual inspection
6.3.4 Alerting	SIEM integration for event alerts; optional Moxa relay for local physical alarms (lights/sirens).
6.3.5 Other controls	Additional zero-trust and session governance features as layered defenses.

Cross-Standard Reinforcement (CIP-005/007/011/013)

CIP-005-5 (Interactive Remote Access)

- **Intermediate System:** CSG is the broker/intermediate system limiting direct access to BES Cyber Systems.
- **Encryption:** Brokered sessions with TLS; entities can terminate/establish encryption at the CSG.
- **MFA:** Enforce MFA for all interactive remote access; supports hardware tokens (e.g., YubiKey).

CIP-007-6 (Ports/Services; Event Monitoring; System Access Controls)

Xona provides detailed session/event logging (success/fail logins, start/end times), supports ≥ 90-day retention, and limits logical access to approved assets/protocols.

CIP-011-2 (Information Protection)

Pixels-only to the endpoint prevents BES Cyber System Information from leaving the ESP into user devices; TLS protects confidentiality in transit.

CIP-013-1 (Supply Chain Risk Management)

Documented processes for monitoring incidents and verifying software integrity/authenticity before updates.

Platform Capabilities for Audit Readiness

Xona delivers the evidence and controls auditors require:

- **Protocol Isolation & Disconnected Access:**

No endpoint-to-asset connectivity; only HTTPS (443) to the CSG eliminates lateral movement paths.

- **Comprehensive Session Evidence:**

Full-fidelity recording and logs for RDP/SSH/VNC with SIEM forwarding and eDiscovery-ready artifacts.

- **Enterprise Identity Integration:**

MFA enforcement including hardware tokens; SAML/AD/LDAP federation; credential injection eliminates shared passwords.

- **Moderated Access Controls:**

Wait room, dual approval, and moderated file transfer with quarantine, scanning, and chain-of-custody tracking.

- **Centralized Management:**

XCM enforces consistent policies, user controls, and logging across distributed CSGs.

- **Air-Gap Friendly:**

On-premises operation with no cloud dependency or "phone home" requirements.

Reference Architectures & Deployment Models

Site-Level Deployment

Deploy a CSG inside the ESP or DMZ, exposing only HTTPS (443) to users' browsers. This eliminates the need for VPN clients, agents, or exposed jump box RDP connections.

Enterprise Management

Utilize Xona Central Manager (XCM) to enforce consistent policies and approvals while aggregating logs across multiple sites.

Rapid Implementation

Deployments typically complete in under 30 minutes per site using virtual appliances or DIN-rail/1U hardware. Large, distributed rollouts have been completed in hours to days, not weeks or months.

Recommended Configuration Blueprint for CIP-003-9 Section 6 Compliance

To achieve full compliance and audit readiness, configure Xona using the following best practices:

1. Identity & MFA

Configuration: Federate with AD/SAML and enforce MFA (hardware token preferred) for all vendor access. Enable credential injection to keep credentials out of vendor hands.

Why this matters: CIP-003-9 requires pre-authorization and positive identification of all vendor access. By federating with your existing identity provider, you maintain a single source of truth for user identities while hardware token-based MFA provides non-repudiable authentication evidence. Credential injection eliminates the risks associated with shared passwords and ensures vendors never possess permanent credentials to your critical systems.

2. Authorization (RBAC/TBAC)

Configuration: Map vendors to named accounts and specific assets. Enforce time-bounded access with zero standing privileges. Require moderation and dual approval for high-risk actions.

Why this matters: Section 6.1.1 mandates documented steps to pre-authorize access on a "time of need" basis. Role-Based and Time-Based Access Control (RBAC/TBAC) ensures vendors can only access authorized systems during approved windows, automatically expiring privileges when work is complete. This eliminates permanent vendor access and creates clear audit trails showing who authorized what access, when, and for how long.

Recommended Configuration Blueprint (continued)

3. Session Oversight & Evidence

Configuration: Enable video recording and comprehensive logs for all vendor protocols. Forward real-time events to your SIEM. Maintain searchable records for at least 90 days (1 year recommended).

Why this matters: CIP-003-9 Section 6.1 requires session monitoring, recording, and logging to demonstrate oversight and enable incident investigation. Full-fidelity video captures every action taken during vendor sessions, providing non-repudiable evidence for auditors and security teams. SIEM integration enables real-time alerting on suspicious activity, while extended retention supports forensic analysis and compliance reporting.

4. Detection & Alerting

Configuration: Configure SIEM forwarding via Splunk, RSyslog, or Generic HTTP. Optionally deploy a Moxa relay for local visual and audible alerts in control rooms.

Why this matters: Section 6.3 requires the ability to detect malicious communications. Real-time event forwarding to your SIEM enables correlation with other security events and automated threat detection. Local alerting provides immediate notification to control room operators when vendors connect, supporting the requirement for active session monitoring and rapid response to anomalies.

5. Disablement Drills

Configuration: Document and rehearse Lockbox (global disable), Kill (immediate session termination), and Edit Connection (protocol-level disable) procedures. Retain runbook evidence and drill records.

Why this matters: Section 6.2 explicitly requires documented processes to immediately disable vendor electronic remote access, including ports, services, and protocols. Regular drills ensure your team can execute emergency disconnection procedures under pressure. Documented runbooks and drill records demonstrate to auditors that you maintain operational readiness to sever vendor access within seconds of detecting malicious activity or policy violations.

6. File Governance

Configuration: Require moderated file transfer with malware scanning and approval workflows. Preserve complete chain-of-custody documentation for all file movements.

Why this matters: Section 6.3.1 addresses anti-malware controls for detecting malicious communications. Uncontrolled file transfers are a primary malware vector into OT environments. Moderated file transfer with mandatory scanning creates a security checkpoint where every file is inspected and approved before entering your critical systems. Chain-of-custody records prove that files were vetted and authorized, providing critical evidence during audits and incident investigations.

Implementation Note: These six configuration areas work together to create a defense-in-depth posture that satisfies CIP-003-9 Section 6 requirements while materially reducing your operational risk and compliance burden. Each capability generates the artifacts auditors expect to see: pre-authorization records, session evidence, detection capabilities, and documented procedures for emergency response.

Why Replace VPNs and Jump Servers **Before April 1, 2026**

CIP-003-9 Section 6 requires tight control and comprehensive visibility over vendor remote access. Traditional VPNs and jump servers expand your attack surface, complicate MFA implementation and logging, and leave critical gaps in supervision and audit evidence.

Xona was purpose-built to replace these legacy stacks with a hardened, agentless platform that prevents lateral movement, simplifies audit preparation, and reduces compliance risk—all while improving operational efficiency.

Take the Next Step

Ready to evaluate Xona for your CIP-003-9 implementation? [Contact us](#) for a technical walkthrough and compliance mapping session tailored to your environment.

About Xona Systems

Xona Systems provides Zero Trust secure remote access built specifically for operational technology and critical infrastructure environments. The Xona Platform replaces VPN-based access with identity-driven, least-privilege control, full session visibility, and audit-ready accountability, without exposing OT networks or disrupting operations. www.xonasystems.com