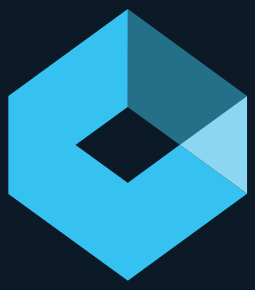
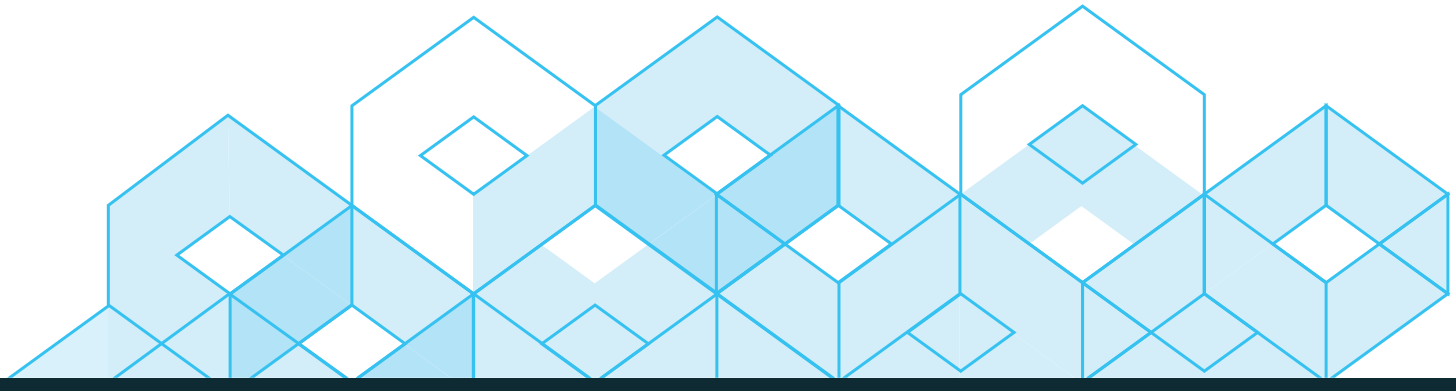


xage
SECURITY

WHITEPAPER

Navigating NERC CIP Requirements with Xage

Table of Contents



xage SECURITY

Introduction: Why NERC CIP Is Changing—and Who Is Affected

The North American Electric Reliability Corporation (NERC) periodically updates its Critical Infrastructure Protection (CIP) standards to keep pace with evolving threats to the Bulk Electric System (BES). Over the next one to two years, CIP-003-9, CIP-005-7, CIP-010-4, and CIP-013-2 are slated for 2024–2025 enforcement. These updates introduce revised requirements that can significantly affect Transmission and Distribution (T&D) operators, Generation owners, and other Registered Entities. Two primary drivers stand out:

- **Increased Threat Landscape:** Cyber threats targeting the power sector have escalated in sophistication and frequency. Nation-state actors, organized cybercriminals, and insiders exploit vulnerabilities in IT and OT (operational technology) systems alike. To counter these threats, regulators are tightening or clarifying existing security controls, particularly around remote access, vendor oversight, and configuration management.
- **Refined BES Cyber System (BCS) Categorization:** CIP-002 sets the foundation for determining whether assets are classified as Low, Medium, or High Impact. However, new thresholds, definitions, and clarifications—especially in CIP-003-9—are effectively re-categorizing some assets to higher impact levels or mandating more robust requirements for sites that remain Low Impact. This means that some smaller or previously less-regulated assets now face tougher security measures, such as more detailed access controls, enforced logging, and multi-factor authentication (MFA).

Who Is Affected?

- **Transmission & Distribution Utilities:** Substations and control centers, which may have previously fallen under Low Impact, are now being re-evaluated for potential higher impact classifications—or face stronger Low Impact requirements.
- **Generation Owners & Operators:** Facilities with DERs (Distributed Energy Resources) or expanded interconnections may discover their reliability influence has grown, thus placing them under more stringent CIP demands.
- **Balancing Authorities & Reliability Coordinators:** Entities already at Medium or High Impact will see revised or clarified requirements for remote access, device protections, and vendor oversight.
- **Vendors & Service Providers:** CIP-013-2 supply chain requirements introduce stricter rules for third-party access, making vendor practices a focal point for compliance reviews.

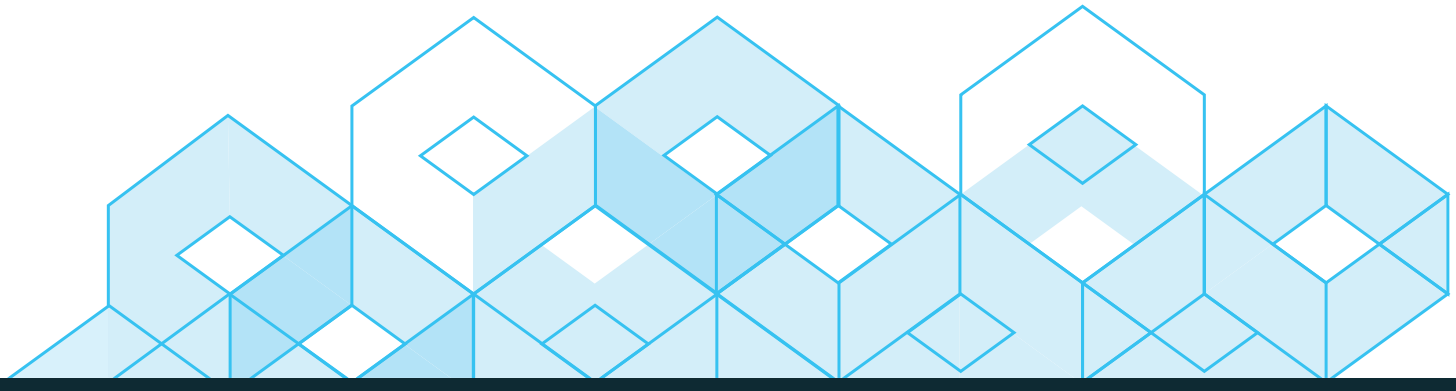
Expanded Scope for Low Impact Systems

Historically, entities with Low Impact BES Cyber Systems (BCS) faced relatively fewer compliance obligations. However, CIP-003-9 significantly increases the rigor for Low Impact sites, narrowing the gap between Low and Medium Impact practices.

Key areas of expansion include:

- **Remote Access Oversight:** Low Impact facilities now must document and enforce stricter controls on external routable connectivity. In many cases, MFA—once primarily associated with Medium or High Impact environments—will be required for interactive remote access at Low Impact sites.
- **Enhanced Logging Expectations**: While previous Low Impact requirements emphasized minimal security management and reporting, CIP-003-9 calls for more detailed logs and audits of critical actions or events. This aligns with the Medium Impact standard of providing deeper visibility into who is accessing systems and when changes occur.
- **Alignment with Medium Impact Practices:** CIP-003-9 encourages Low Impact sites to adopt what are effectively "medium-level" controls, including stronger authentication, heightened supply chain scrutiny, and more comprehensive documentation of their security posture.
- **Distributed Energy Resources (DERs):** The growing integration of DERs at distribution or substation levels means that even a small site can have a significant impact on grid stability. Where substations interact with advanced generation assets (solar, wind, batteries, microgrids), NERC CIP standards increasingly view these as critical points in the Bulk Electric System.

As a result of these shifts, **organizations that once treated Low Impact sites as relatively simple to secure may need to reassess their strategies for substation security, remote access management, and vendor control.** Ensuring compliance with CIP-003-9 means proactively strengthening cybersecurity measures—often matching or closely paralleling the controls found in Medium Impact settings.



xage SECURITY

Challenges with the New NERC CIP Categorization

The updated NERC CIP standards are prompting a reassessment of asset classifications across the electric grid, particularly at Transmission and Distribution (T&D) substations. While some facilities may remain Low Impact, the scope and depth of security controls required for Low Impact BES Cyber Systems have increased substantially. In many cases, these newly extended requirements mirror those traditionally reserved for Medium Impact or higher. Below, we explore four key challenge areas facing utilities.

Re-Evaluation of T&D Substations

Traditionally, many T&D substations were classified as Low Impact under CIP-002 due to their perceived minimal risk to Bulk Electric System (BES) reliability. However:

- **Potential Reliability Impact:** Even smaller substations can become critical if they can island (operate independently during grid disturbances) or supply significant local loads.
    - **Example:** A substation supporting a large industrial complex or hosting a microgrid could have a far greater reliability role than previously recognized.
- **Near-Medium Obligations:** As regulators refine the criteria for BES Cyber System categorization, Low Impact may no longer be a suitable label for certain sites. Some substations are thus moving to, or nearing, Medium Impact requirements—which demand more rigorous security controls, including robust perimeter defense, MFA, and heightened logging.

Multi-Factor Authentication (MFA) Expansion

A centerpiece of CIP-005-7 is its emphasis on interactive remote access control, which now requires:

- **Two or More Factors:** This usually involves a combination of something you know (password/PIN), something you have (smart card, token, phone), and/or something you are (biometric). CIP-005-7 specifically calls for strong authentication measures such as smart cards (PKI) or hardware tokens.
- **Applicability at Low Impact Sites:** Unlike previous CIP iterations where MFA was primarily a Medium/High Impact requirement, CIP-005-7 clarifies that external routable connectivity at Low Impact facilities should also implement robust MFA.
    - **Example:** A small substation with remote visibility or control paths may now need a PKI-based login system, even if it lacks a full CIP-005 High/Medium classification.

MFA Requirement	Previous Practice	Under CIP-005-7
Applicability	Required mainly for Medium/High Impact facilities	Expanded to Low Impact where external routable connectivity exists
Implementation	Username/password or partial MFA solutions	Strong MFA with PKI, smart card, or equivalent (two-factor minimum)
Enforcement & Evidence	Often handled ad-hoc or with limited logging	Mandatory logging and tracking of all interactive remote sessions

New Requirements for Configuration & Supply Chain

Beyond access control, the updated standards target configuration management and vendor risk with a sharper focus:

- **CIP-010-4 (Configuration & Vulnerability Management)**
  - **Secure Patching & Tracked Config Changes:** Entities must ensure that every software or firmware update is authorized, verified, and recorded.
  - **Vulnerability Assessments:** Regular checks are now extended to a broader group of systems, potentially including devices once classified as Low Impact.
- **CIP-013-2 (Supply Chain Risk Management)**
  - **Deeper Vendor Oversight:** Any system that can affect the BES (directly or indirectly) must enforce secure file transfers, remote sessions, and robust contractual obligations for third-party providers.
  - **Examples:** Firmware upgrades from an OEM vendor or maintenance access by a third-party integrator must be tightly controlled, with logs and session details available for audit.

Requirement	Key Focus	Impact on Utilities
CIP-010-4	Patch management, changes	More devices covered; stricter logging of config changes & vulnerability scans
CIP-013-2	Supply chain security	Vendors, OEMs, integrators must follow secure delivery & remote service rules

Audit & Evidence Burden

Finally, logging, session recording, and event tracking requirements continue to tighten under newer CIP versions:

- **Mandatory Logging for Low Impact BCS:** While logs and alerts were once seen as primarily Medium/High Impact obligations, Low Impact sites under CIP-003-9 are expected to maintain more thorough records of critical activities.
- **Potential Noncompliance Risks:** Failure to provide timely, detailed logs for remote sessions, configuration changes, or incident handling can open utilities to compliance violations or financial penalties.
    - This burden increases significantly when substation networks lack centralized logging or a standardized approach to capturing activity from diverse devices (IEDs, RTUs, relays, etc.).

How Xage Helps Address New NERC CIP Requirements

To meet the existing as well as new 2024–2025 NERC CIP updates (CIP-003-9, CIP-005-7, CIP-010-4, CIP-013-2), utilities need end-to-end controls that strengthen remote access, vendor oversight, and device security. Xage provides zero trust access and protection that ties device identity, smart card/PKI authentication, micro-segmentation, secure file transfer, and privileged session recording into a single, policy-driven platform.

Below, we outline core capabilities of the Xage Platform and how each directly supports CIP compliance.

Xage Capability	Description	Relevant CIP Standards	Key Benefit
PKI-Based MFA (Smart Card/CAC/PIV)	Enables multi-factor authentication using physical PKI tokens (e.g., YubiKey, CAC, or PIV) for interactive remote sessions.	**CIP-005** for MFA **CIP-003-9** for Low Impact with external connectivity	Ensures strong identity verification for remote access Protects against password theft and replay attacks Meets new Low Impact requirements for multi-factor under CIP-005 style rules
Role & Policy Mapping	Integrates with existing PKI/CA infrastructures (e.g., Microsoft CA) or SAML/LDAP for single sign-on. Each certificate maps to a unique identity in Xage, allowing role-based (or task-based) access enforcement.	**CIP-005** (Remote Access) **CIP-013** (Vendor Oversight)	Simplifies credential management and least-privilege controls Centralizes user provisioning and deprovisioning

Xage Capability	Description	Relevant CIP Standards	Key Benefit
Session Recording & Command Control	Logs and records all privileged sessions (SSH, RDP, HTTP/HTTPS). Ties each action or command to a specific user identity.	**CIP-005** (Remote Logging) **CIP-010** (Evidence of Changes)	Provides audit-ready evidence of who did what Streamlines incident forensics, preventing CIP noncompliance
Fine-Grained Privilege Assignment	Allows operators to define permissible commands or actions for each role, preventing unauthorized changes to critical devices or ICS networks.	**CIP-003-9** (Expanding Low Impact Controls) **CIP-005**	Enforces granular "who can do what" Demonstrates robust control even at Low Impact sites
Device Identity & Micro-Segmentation	Enrolls each ICS/OT device (relay, IED, RTU, server) into the Xage Fabric, assigning a cryptographic identity. Implements a "deny by default" policy for device-to-device traffic.	**CIP-005** (Electronic Security Perimeter) **CIP-003-9**	Ensures only trusted devices communicate Minimizes lateral movement if one device is compromised
Granular Connection Rules	Administrators specify which protocols (DNP3, Modbus, IEC 61850) are allowed between devices, blocking all other communication paths.	**CIP-005** (ESP & Communication Paths)	Eliminates unauthorized channels Reduces risk of CIP violations or advanced persistent threats moving laterally
Secure File Transfer (Encrypted Channel)	Provides a secure, logged channel for distributing patches, firmware, and config updates. Tracks who sends files, to which device, and when.	**CIP-010-4** (Config & Patch Management) **CIP-013-2** (Supply Chain)	Prevents tampering or man-in-the-middle attacks Facilitates authorized updates and patch delivery
Vendor-to-Utility Collaboration	Grants time-bounded or role-limited file transfer/upload privileges to third-party OEMs or integrators.	**CIP-013-2** (Vendor Oversight)	Controls external partner activities Ensures patches/software come from verified sources only
Automated Change Audit Trails	Links every file transfer or config change to a user identity (via PKI certificate). Captures cryptographic checksums for integrity.	**CIP-010** (Evidence of Changes) **CIP-005**	Single source of truth for "what changed, who changed it, when" Critical for demonstrating compliance during audits

xage SECURITY

Xage Capability	Description	Relevant CIP Standards	Key Benefit
Single Pane of Glass (Centralized Logging)	Aggregates logs and session data from users, devices, file transfers, and policy enforcements into one central repository.	**CIP-005** (Logging) **CIP-003-9** (Low Impact Logging)	Simplifies auditing by consolidating evidence Reduces time to gather data for CIP compliance or incident response
Real-Time Alerts & Correlation	Generates alerts for anomalous behaviors (e.g., vendor attempts to access an unapproved device). Can integrate with SIEM solutions for correlation.	**CIP-008** (Incident Reporting)	Rapid detection of unauthorized actions Accelerates incident response, reducing potential CIP violations
Session Replay & Forensics	Captures full command logs (screens viewed, keystrokes) for thorough post-incident analysis.	**CIP-010** (Investigations) **CIP-005** (Remote Session Audits)	Provides indisputable record of changes Ensures quick root-cause identification and CIP compliance
Compliance Reporting & Analytics	Offers built-in tools to retrieve logs by user, device, time range, or CIP requirement, easing compliance workflows.	**CIP-005 & CIP-003-9** (Enhanced Low Impact Logging)	Reduces manual data gathering for audits Delivers on-demand proof of compliance for regulators

Benefits of Adopting Xage for Re-Categorized & Low Impact Assets

Uniform Protection Across All Impact Levels

As regulatory thresholds evolve and more assets move from Low to Medium Impact (or face enhanced Low Impact obligations), Xage ensures a consistent, high-integrity security posture across the board.

- **Scalable Security:** Whether a substation is newly designated as Medium Impact or still classified as Low Impact, Xage applies the same zero trust controls—PKI-based MFA, micro-segmentation, and session monitoring—minimizing gaps in coverage.
- **Eliminate Patchwork Solutions:** Utilities avoid retooling each time an asset's status changes; a single Xage deployment can be extended or adjusted via policies rather than requiring new hardware or separate software installations.

Lower Operational Overhead

Traditional or legacy security solutions, such as hardware VPNs and ad-hoc RDP setups, can be both resource-intensive and difficult to manage at scale. Xage's approach significantly reduces complexity:

- **Browser-Based Remote Access:** Engineers and vendors can securely connect using PKI credentials via a standard web interface, rather than juggling multiple VPN clients or hardware tokens.
- **Centralized Configuration:** A single, policy-driven Xage Fabric streamlines access management, patch delivery, and logging, minimizing the need for IT teams to maintain disparate systems at each site.

Streamlined Audit Readiness

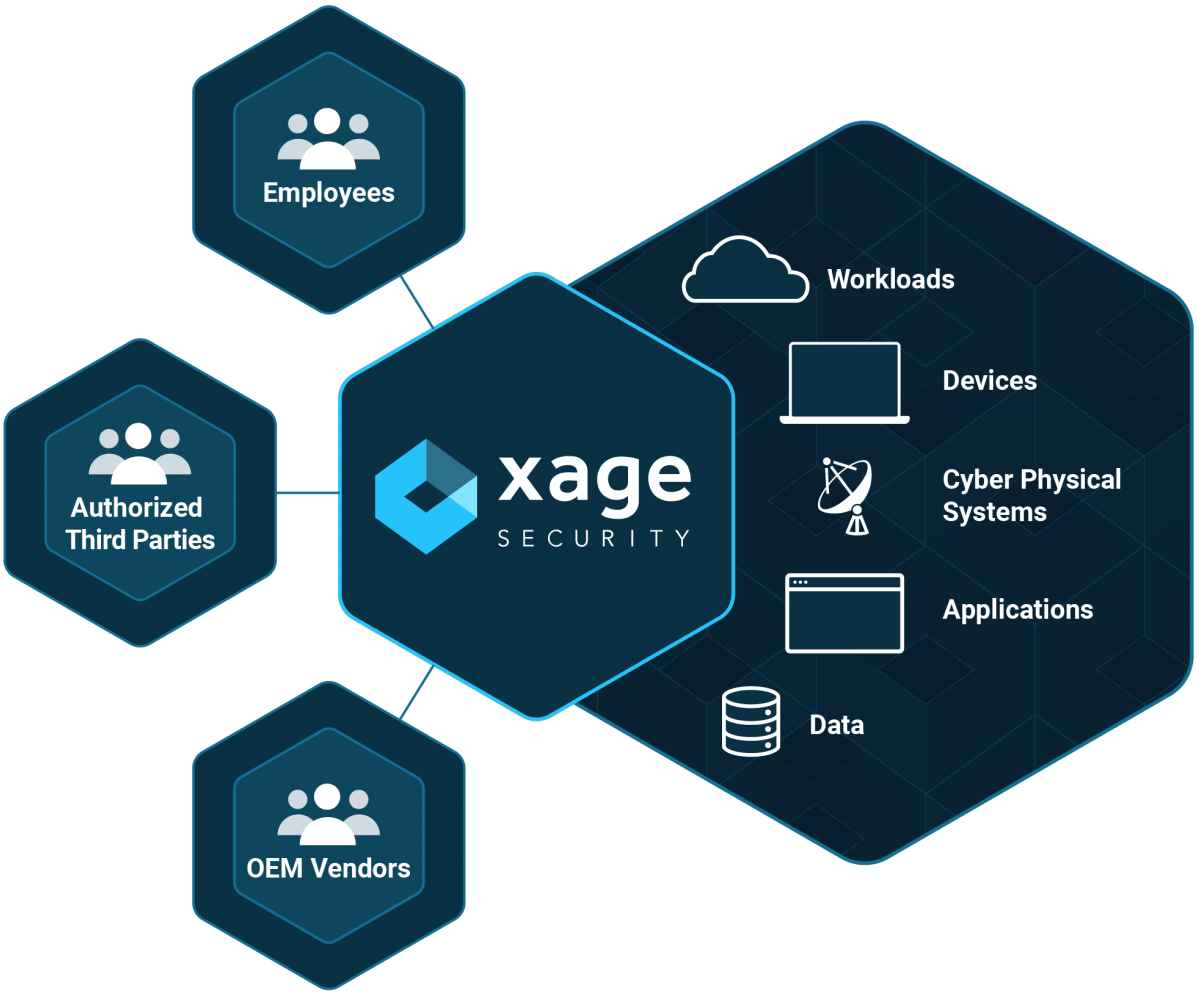
Proving compliance under CIP-003-9, CIP-005, CIP-010, and CIP-013 can be cumbersome, especially if logs and access records are scattered across various tools. Xage alleviates this audit burden:

- **Single Repository:** All session data, file transfers, and device-to-device communications are captured in one central log, making it easy to retrieve and correlate events for audits or incident reviews.
- **Time-Savings for Compliance Teams:** Instead of manually piecing together evidence from different platforms, compliance teams can quickly export or review logs that are already mapped to specific CIP requirements.

Future-Proof Against Evolving NERC CIP Mandates

The NERC CIP environment remains dynamic, with ongoing revisions and new standards (e.g., CIP-003-9's newly clarified Low Impact measures, CIP-005-7's extended remote access rules). Xage keeps pace:

- **Zero Trust & Identity-Centric:** Xage's architecture is policy-driven, allowing utilities to tweak configurations or add new policies without forklift upgrades whenever CIP standards evolve.
- **Adaptive, Modular Approach:** Because Xage is built around device identities and role-based controls, implementing future updates—like stricter vendor oversight or expanded vulnerability assessments—requires minimal reconfiguration of the existing platform.



About Xage Security

Xage is a global leader in zero trust access and protection on a mission to pioneer a secure tomorrow. Control access and prevent attacks in the cloud, in the data center, at the remote operational edge anywhere on Earth, and even in orbit with the Xage Fabric Platform. Xage is easy to manage and can be deployed in a day, giving users easy and secure access to the assets they need from anywhere, while preventing advanced adversaries and insider threats at every stage of the attack chain. Learn why organizations like the U.S. Space Force, PETRONAS, and Kinder Morgan choose Xage at xage.com.