Xage Security for NERC CIP-003-11

Strengthening Low Impact BES Cyber System Access With Identity-Centric Zero Trust

CIP-003-11 is the latest revision to NERC's Security Management Controls standard. Although the standard continues to address governance and accountability requirements for BES Cyber Systems, the most significant practical change is its **sharpened focus on Low Impact BES Cyber Systems and the way electronic access into those environments is controlled.** The revision clarifies that access controls are not limited to a higher-level network boundary; they must be enforced where routable access reaches the Low Impact BES Cyber System environment itself, including the relevant low impact asset perimeter and supporting shared cyber infrastructure. FERC approved CIP-003-11 on March 19, 2026, and NERC's implementation plan gives Responsible Entities a 36-month transition period following regulatory approval to modernize low impact access architectures and strengthen authentication, access governance, and control over vendor connectivity.

Why this update matters

CIP-003-11 reflects the industry's recognition that low impact sites can still create meaningful system-wide risk, especially when many distributed assets are reached through inconsistent remote access, weak authentication, and loosely governed vendor connectivity. The revised standard pushes utilities toward tighter control over who can connect, what they can reach, and how those connections are governed, monitored, and revoked.

Low Impact BES Cyber Systems *are in-scope BES Cyber Systems that do not meet the High or Medium Impact criteria under CIP-002, but still support reliable Bulk Electric System operations and remain subject to applicable low impact CIP controls. Typical examples include* ***Smaller transmission stations and substations, Lower-threshold generation sites, blackstart and cranking path facilities, and certain protection systems qualifying Distribution Provider assets.***

For utilities, this is not simply a policy update. It is an access architecture issue. The standard now places more emphasis on necessary electronic access, user authentication before access is granted, protection of authentication information in transit, and stronger operational control over vendor electronic access. That is where Xage aligns naturally.

The Xage architectural model for utilities

Xage helps utilities modernize low impact access without forcing a tradeoff between security and operational usability. The platform provides browser-based and native application access, identity-based policy control, multi-factor authentication, centralized vendor governance, secure file transfer, and distributed enforcement across layered OT environments. Instead of extending trust across the network, Xage brokers and enforces access at each step.

Identity-centric Access

Granular policy control down to individual OT assets and applications instead of broad tunnel-based reach.

Multi-hop enforcement

Session and protocol termination at each network boundary to preserve segmentation and reduce lateral movement risk.

Audit-quality visibility

Tamper-proof logs, session recording, and analytics-ready data to support compliance and operational review.

How Xage aligns to the core CIP-003-11 focus areas

CIP-003-11 control theme	What the standard is driving toward	How Xage helps
Necessary electronic access	Permit only the inbound and outbound electronic access that is actually needed for low impact environments.	Xage replaces broad VPN-style reachability with identity-based, least-privilege access to specific OT assets and applications. Utilities can grant access to only the systems, sessions, and tools required for the task at hand.
User authentication before access	Authenticate each user before allowing access into the network that contains low impact BES Cyber Systems or supporting shared infrastructure.	Xage supports pre-access authentication with SSO, MFA, and policy enforcement before a user is allowed deeper into the environment. MFA can also be applied again at later layers, assets, or applications when needed.

CIP-003-11 control theme	What the standard is driving toward	How Xage helps
Protection of authentication data in transit	Protect user authentication information as credentials, tokens, and session initiation data move across the access path.	Xage uses encrypted access flows and controlled authentication paths, reducing exposure of credentials across remote access, contractor access, and support workflows.
Vendor electronic access visibility	Maintain a reliable method for determining when vendor electronic access is occurring.	Xage provides centralized visibility through just-in-time access, session monitoring, session recording, and tamper-proof audit logs that show who accessed what, when, and under what policy.
Vendor access control and revocation	Maintain a method for disabling vendor electronic access when it is no longer needed or should not be active.	Xage enables centralized policy control, time-bounded authorization, and rapid revocation of vendor access without exposing broad network connectivity.
Evidence and operational traceability	Maintain defensible records that support internal review, investigations, and compliance validation.	Xage generates tamper-proof audit records, policy-driven session recordings, and analytics-ready visibility that strengthen audit readiness and post-event reconstruction.

Recommended Xage deployment pattern for low impact environments

For utilities preparing for CIP-003-11, Xage is most effective as the identity-centric access layer in front of low impact BES Cyber System environments. In that role, Xage helps enforce least-privilege access, authenticate users before they are allowed into protected networks, govern and revoke vendor access, preserve segmentation across layered environments, and generate the audit-quality evidence that regulated operators need for internal review and compliance support. The result is a more controlled and more defensible access model for distributed utility operations: one that improves day-to-day security while also aligning closely to the technical intent of the revised low impact access requirements.

Users and third parties

Employees, OEMs, integrators, and maintenance providers initiate access through browser-based or native application workflows.

Xage identity and policy layer

SSO, MFA, JIT authorization, session policy, vendor governance, and secure file movement are enforced before broader access is allowed.

Layered OT environment

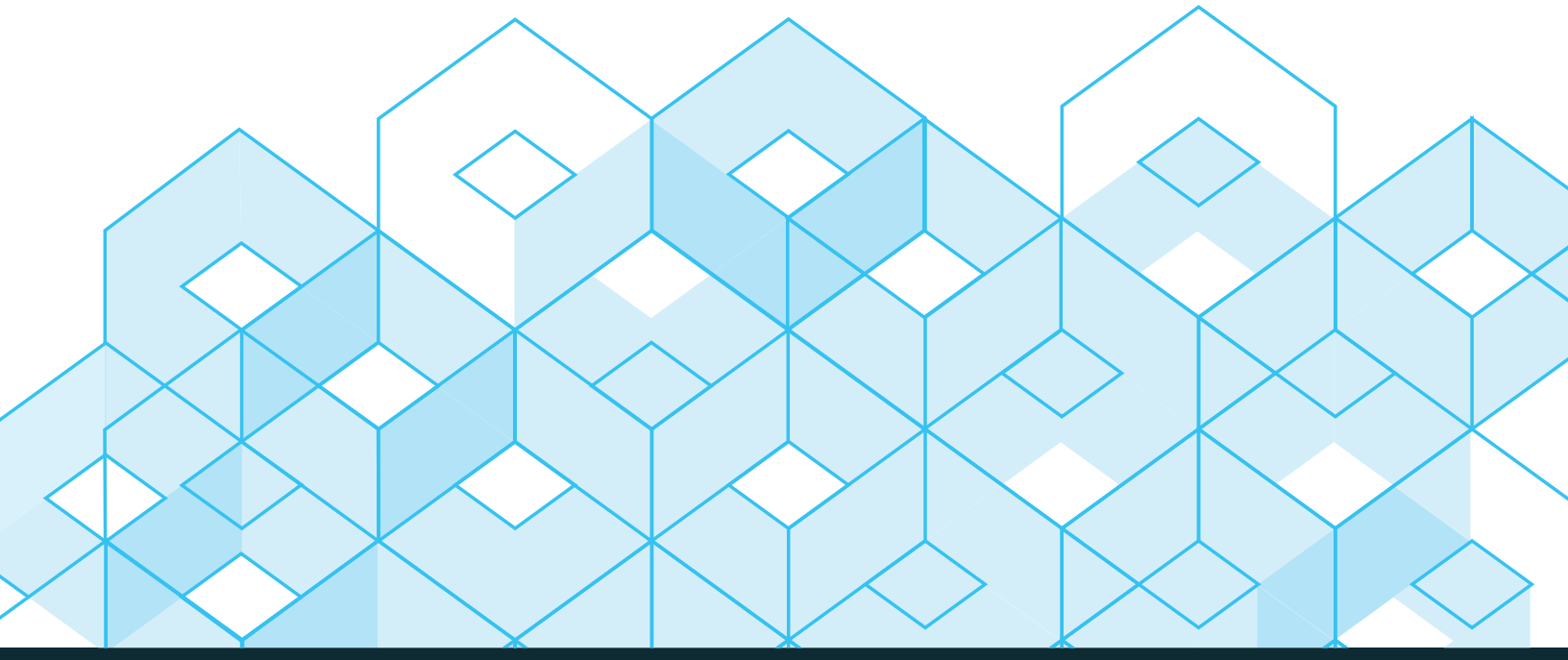
Multi-hop session and protocol termination preserve segmentation as access moves through the DMZ and network layers to the authorized target.

What utilities gain with Xage in this part of the program

Replace broad VPN trust	Xage moves access decisions from the network layer to the identity, asset, and session layer, which is far better aligned to the intent of CIP-003-11.
Preserve layered OT segmentation	Xage's multi-hop architecture supports protocol and session termination at each boundary, helping utilities maintain defense-in-depth across IT, DMZ, control center, and field environments.
Govern contractor and OEM access	Xage gives utilities a consistent operating model for vendors, integrators, relay specialists, and remote support teams through just-in-time access, strong authentication, and clear audit trails.
Support monitored file movement	Xage enables controlled, encrypted file transfer with malware scanning and integrity verification for engineering files, configuration packages, and supporting data moving across IT, DMZ, and OT layers.

About Xage Security

Xage Security 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. Visit xage.com to learn more.



xage SECURITY