Cyolo

How Cyolo Helps You Achieve Compliance: NERC CIP

The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) plan is a set of standards aimed at regulating, enforcing, monitoring and managing the security of Bulk Electric System (BES). The NERC CIP standards are required by law and govern critical infrastructure of all entities that substantively impact the reliability of BES, including owners, operators, and users of these systems. To comply with NERC CIP, utility companies in North America must adhere to a baseline set of cybersecurity measures that include enabling security controls, performing risk analysis, and governing access to critical assets.

Cyolo can help companies comply with NERC CIP by providing granular access control, multi-factor authentication, encryption, continuous monitoring, and compliance reporting capabilities. These solutions help companies to implement effective security controls to protect BES.

HERE ARE SOME WAYS THAT CYOLO SUPPORTS NERC CIP COMPLIANCE:

Access Management: Cyolo manages user identities and access, ensuring that only authorized users can access systems and resources.

Access Control: Cyolo provides dynamic, context-based access control policies that can adapt to changing circumstances, such as the user’s location, device type, and the sensitivity of the information being accessed.

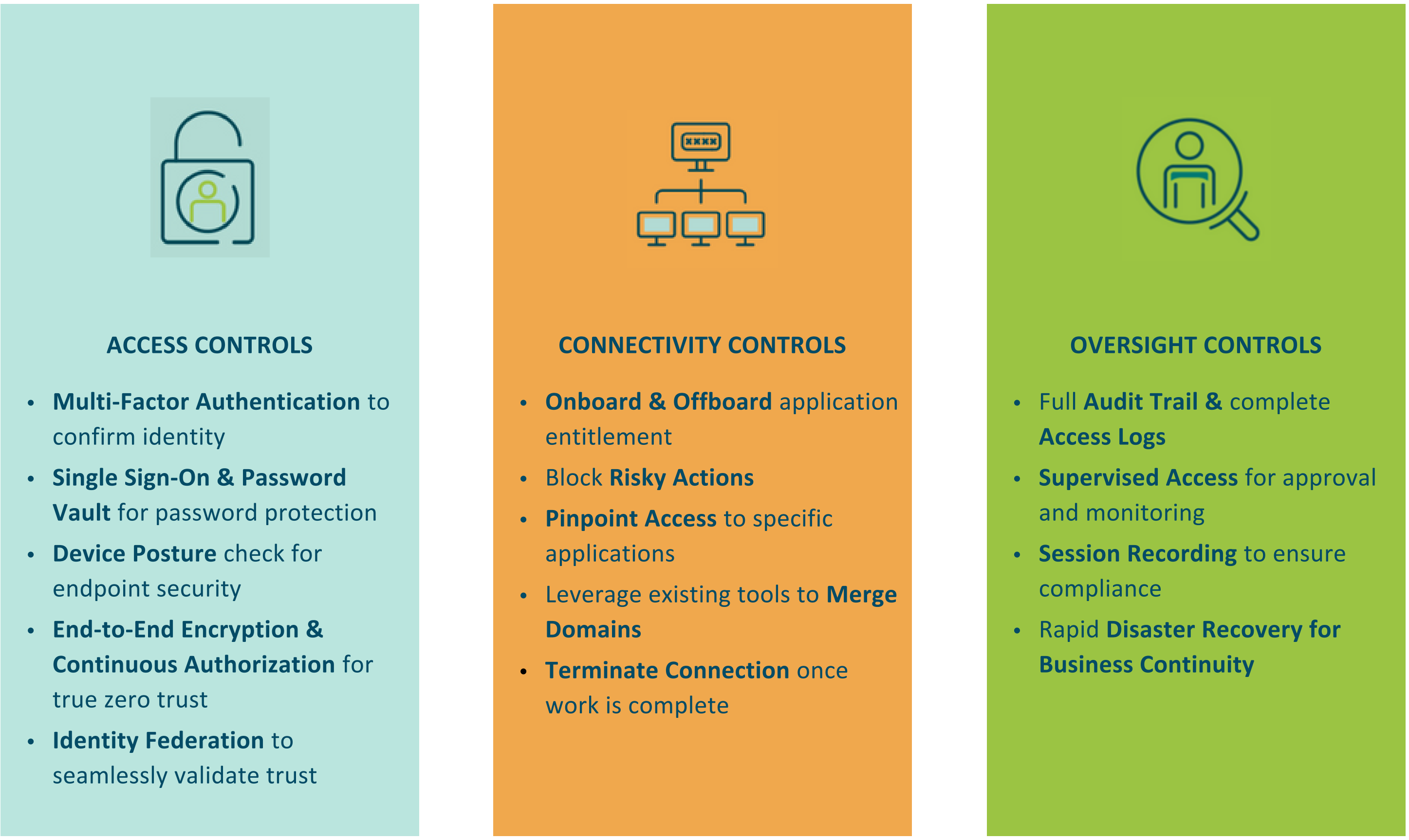
With its zero-trust access solution, Cyolo delivers three layers of controls to better manage scenarios in which user access could cause enormous damage to the business. Deploying Cyolo materially helps support NERC CIP compliance.

Secure Remote Access (SRA): Cyolo enables zero-trust access for all users, regardless of their location, and is both faster and more secure than traditional SRA solutions like virtual private networks (VPNs).

Visibility and Continuous Monitoring: Cyolo continuously monitors and logs user activity to ensure that systems and resources are being accessed and used in accordance with applicable policies and regulations.

HOW CYOLO HELPS

Cyolo is designed to give users access to the resources they need while maintaining the zero-trust model. It is built to support the real world, allowing companies to protect their entire network. With Cyolo, you can securely access the resources you need to get your work done, while keeping your network and data safe.



ACCESS CONTROLS

- **Multi-Factor Authentication** to confirm identity
- **Single Sign-On & Password Vault** for password protection
- **Device Posture** check for endpoint security
- **End-to-End Encryption & Continuous Authorization** for true zero trust
- **Identity Federation** to seamlessly validate trust

CONNECTIVITY CONTROLS

- **Onboard & Offboard** application entitlement
- Block **Risky Actions**
- **Pinpoint Access** to specific applications
- Leverage existing tools to **Merge Domains**
- **Terminate Connection** once work is complete

OVERSIGHT CONTROLS

- Full **Audit Trail &** complete **Access Logs**
- **Supervised Access** for approval and monitoring
- **Session Recording** to ensure compliance
- Rapid **Disaster Recovery for Business Continuity**

(Figure 1. Cyolo Zero-Trust Access controls that support compliance with NERC CIP)

CYOLO ALIGNMENT WITH NERC CIP

CIP-004-6 – PERSONNEL & TRAINING
5.1 A process to initiate removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action
5.2 For reassignments or transfers, revoke the individual’s authorized electronic access to individual accounts
5.3 For termination actions, revoke the individual’s access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.
5.4 For termination actions, revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.
5.5 For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.
CIP-005-6 – ELECTRONIC SECURITY PERIMETERS
1.1 All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.
1.2 All External Routable Connectivity must be through an identified Electronic Access Point (EAP).
1.3 Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.
1.4 Where technically feasible, perform authentication when establishing Dialup Connectivity with applicable Cyber Assets.
2.1 For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
2.2 For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.
2.3 Require multi-factor authentication for all Interactive Remote Access sessions.
2.4 Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).
2.5 Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).

CIP-007-6 – SYSTEM SECURITY MANAGEMENT
1.1 Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports.
3.1 Deploy method(s) to deter, detect, or prevent malicious code.
4.1 Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents 4.1.1 Detected successful login attempts; 4.1.2 Detected failed access attempts and failed login attempts.
4.2 Generate alerts for security events that the Responsible Entity determines necessitates an alert4.2.2 Detected failure of Part 4.1 event logging.
4.3 Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days
4.4 Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.
5.1 Have a method(s) to enforce authentication of interactive user access, where technically feasible.
5.2 Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).
5.3 Identify individuals who have authorized access to shared accounts.
5.4 Change known default passwords, per Cyber Asset capability
5.5 For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: • **5.5.1** Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and • **5.5.2** Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, nonalphanumeric) or the maximum complexity supported by the Cyber Asset.
5.6 Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.
5.7 Where technically feasible, either: Limit the number of unsuccessful authentication attempts; or Generate alerts after a threshold of unsuccessful authentication attempts.