Cyolo

How Cyolo Helps You Achieve Compliance: NIST 800-171

Achieving NIST 800-171 compliance is necessary for companies that handle Controlled Unclassified Information (CUI) on behalf of the US government. Compliance can provide a range of benefits including improved cybersecurity, customer trust, competitive advantage, and business operations. The framework is based on the principle of continuous monitoring and improvement, which requires organizations to continually assess and manage risks to CUI and to adapt their security controls to address emerging threats and vulnerabilities.

Cyolo can help companies comply with NIST 800-171 by providing granular access control, multi-factor authentication (MFA), encryption, continuous monitoring, and compliance reporting capabilities. These solutions help companies to implement effective security controls to protect CUI and to demonstrate compliance with applicable regulations and standards.

HERE ARE SOME WAYS THAT CYOLO SUPPORTS NIST 800-171 COMPLIANCE:

Access Control: Cyolo deploys granular access controls to ensure that only authorized individuals can access CUI. The Cyolo solution 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.

SECURE SOLUTION

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 NIST 800-171 compliance during an audit.

Multi-Factor Authentication: Cyolo implements MFA to ensure that individuals are properly identified and authenticated before being granted access to CUI.

Encryption: Cyolo encrypts data from end-to-end and does not decrypt the traffic in its cloud. This makes Cyolo a true zero-trust access solution that is ideal to protect CUI in transit and at rest.

Continuous Monitoring: Cyolo continuously monitors and logs user activity to ensure that CUI is 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, enabling 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**
- Control **Activity Permissions**
- **Terminate Connection** once work is completed

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 NIST 800-171)

CYOLO ALIGNMENT WITH NIST 800-171

ACCESS CONTROL
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.
3.1.3 Control the flow of CUI in accordance with approved authorizations.
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.
3.1.6 Use non-privileged accounts or roles when accessing non-security functions
3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
3.1.8 Limit unsuccessful logon attempts.
3.1.11 Terminate (automatically) a user session after a defined condition.
3.1.12 Monitor and control remote access sessions.
3.1.14 Route remote access via managed access control points.
3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.
3.1.20 Verify and control/limit connections to and use of external systems.
AUDIT & ACCOUNTABILITY
3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity
3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.
3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
3.3.9 Limit management of audit logging functionality to a subset of privileged users.
Configuraiton Management
3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.
3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.
3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

IDENTIFICATION & AUTHORIZATION
3.5.1 Identify system users, processes acting on behalf of users, and devices.
3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
3.5.6 Disable identifiers after a defined period of inactivity.
3.5.8 Prohibit password reuse for a specified number of generations.
3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.
3.5.10 Store and transmit only cryptographically protected passwords
3.5.11 Obscure feedback of authentication information
MAINTENANCE
3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.
SYSTEM & COMMUNICATION PROTECTION
3.13.01 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems
3.13.08 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
3.13.09 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
3.13.15 Protect the authenticity of communications sessions