Access Control (3.1) Family

Security Requirements and the Technologies That Implement Them

A practitioner reference for Defense Industrial Base contractors · Family 1 of 14 in a 14-part series on the NIST SP 800-171 families · Prepared July 2026

Overview of the Access Control Family

Access Control (3.1) is the largest and arguably most foundational of the fourteen NIST SP 800-171 Rev 2 security requirement families. It governs **who** and **what** may reach a system, **which** actions they may perform once there, and **how** Controlled Unclassified Information (CUI) is allowed to move within and out of the environment.

The family contains **22 security requirements** - **2 Basic** (from FIPS 200) and **20 Derived** (from NIST SP 800-53). Because so many are identity- and network-centric, a well-designed identity provider and a segmented CUI enclave satisfy a large share of the family at once. This is **Family 1 of 14** in a planned series covering all fourteen 800-171 families.

Which revision applies? This guide covers **NIST SP 800-171 Revision 2**, which is the baseline the DoD's CMMC program and DFARS 252.204-7012 currently require. In May 2024 NIST published **Revision 3**, which reorganizes Access Control (renumbering it to the 03.01 family, consolidating or withdrawing several controls, and introducing organization-defined parameters). Revision 3 has **not** been adopted for CMMC as of this writing - continue to assess against Revision 2 until the DoD formally transitions, and treat Revision 3 as forward-looking.

Requirement wording below is **summarized for readability**. The controlling text is the official publication, **NIST SP 800-171 Rev 2** (security requirements) and **NIST SP 800-171A** (assessment objectives); consult them for exact language. SPRS point values are per the **DoD Assessment Methodology** (NIST SP 800-171 DoD Assessment Methodology, Rev 2).

The 22 Access Control Requirements and Expected Evidence

The evidence column lists the artifacts an assessor typically expects; most controls need **both** a written policy and a technical artifact. The figure under each control ID is its **SPRS point value** (5, 3, or 1) - the score deducted if the control is not met.

NIST SP 800-171 Rev 2 Access Control (3.1) requirements, SPRS weight, and expected evidence.

Control	Security Requirement	Evidence / Artifacts an Assessor Expects
3.1.1 5 pts	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Access control policy; authorized user/device inventory and authorization records; IdP directory config; MFA / Conditional Access policy export
3.1.2 5 pts	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Role-based access (RBAC) definitions; permission/authorization matrix; directory group-membership export
3.1.3 1 pt	Control the flow of CUI in accordance with approved authorizations.	Information-flow policy; firewall rulesets / ACLs; DLP and CASB configuration; network diagram showing CUI flows
3.1.4 1 pt	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Separation-of-duties matrix; role definitions; approval-workflow config showing requester is not the approver
3.1.5 3 pts	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Least-privilege policy; privileged-account inventory; PAM / just-in-time config; periodic access-review records
3.1.6 1 pt	Use non-privileged accounts or roles when accessing nonsecurity functions.	Policy requiring non-privileged accounts for routine work; evidence of separate admin vs. standard accounts
3.1.7 1 pt	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Endpoint privilege-management config; audit logs capturing privileged-function execution; SIEM records
3.1.8 1 pt	Limit unsuccessful logon attempts.	Account-lockout policy setting (GPO / Entra) with threshold and duration; configuration export or screenshot
3.1.9 1 pt	Provide privacy and security notices consistent with applicable CUI rules.	Approved logon-banner text; screenshot of the banner at login; policy referencing the CUI notice
3.1.10 1 pt	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	Session-lock / screensaver GPO or Intune config; screenshot showing pattern-hiding lock and the inactivity timeout
3.1.11 1 pt	Terminate (automatically) a user session after a defined condition.	Session-termination configuration (VPN / application idle timeout); config export

Control	Security Requirement	Evidence / Artifacts an Assessor Expects
3.1.12 5 pts†	Monitor and control remote access sessions.	Remote-access policy; VPN / ZTNA connection logs; SIEM monitoring of remote sessions
3.1.13 5 pts†	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	VPN / TLS configuration using FIPS-validated cryptography; FIPS 140 validation certificate reference
3.1.14 1 pt	Route remote access via managed access control points.	Network diagram showing managed access-control points; gateway / VPN config; firewall rules routing remote access
3.1.15 1 pt	Authorize remote execution of privileged commands and remote access to security-relevant information.	PAM / bastion configuration; MFA on privileged remote access; authorization records for privileged commands
3.1.16 5 pts†	Authorize wireless access prior to allowing such connections.	Wireless-authorization policy and approval records; NAC / 802.1X configuration
3.1.17 5 pts†	Protect wireless access using authentication and encryption.	WLAN controller config showing WPA2/WPA3-Enterprise + 802.1X; encryption settings screenshot
3.1.18 5 pts†	Control connection of mobile devices.	Mobile-device policy; MDM enrollment and compliance report; NAC configuration
3.1.19 3 pts	Encrypt CUI on mobile devices and mobile computing platforms.	MDM encryption-enforcement config; BitLocker / FileVault status report per device
3.1.20 1 pt	Verify and control/limit connections to and use of external systems.	External-systems policy; interconnection / usage agreements; firewall or CASB allowlist; BYOD policy
3.1.21 1 pt	Limit use of portable storage devices on external systems.	Removable-media policy; endpoint device-control config; DLP / USB-restriction settings
3.1.22 1 pt	Control CUI posted or processed on publicly accessible systems.	Publicly-accessible-systems policy; content review/approval records; WAF config; scan confirming no CUI is exposed

2 Basic requirements (3.1.1-3.1.2) and 20 Derived requirements (3.1.3-3.1.22). † No points are deducted if the relevant access type (remote, wireless, or mobile) is not permitted in your environment.

Implementing Technologies and How to Configure Them

The systems below are the common building blocks for the family. One system often satisfies several requirements; the identity provider, MFA, SIEM, and MDM form a backbone that touches nearly every control.

Identity Provider / Directory (Active Directory, Microsoft Entra ID)

- Serve as the single authoritative source for all user, service, and device identities; disable standalone/local accounts where possible. *(3.1.1)*
- Enforce role-based access groups so users receive only the transactions and functions their role requires. *(3.1.2, 3.1.5)*
- Maintain separate standard and privileged (admin) accounts for every administrator; never use admin accounts for email or browsing. *(3.1.5, 3.1.6)*
- Configure account-lockout policy - threshold, counter reset, and lockout duration. *(3.1.8)*
- Push logon banners and session-lock/timeout settings via Group Policy or Conditional Access / Intune. *(3.1.9, 3.1.10)*

Multi-Factor Authentication (MFA)

- Require phishing-resistant MFA for all remote access and all privileged actions. *(3.1.12, 3.1.15)*
- Enforce centrally through Conditional Access or policy - not per-application opt-in - so it cannot be bypassed. *(3.1.1)*

Privileged Access Management (PAM)

- Vault privileged credentials; require check-out with approval and full session recording. *(3.1.5, 3.1.7, 3.1.15)*
- Grant privileged access just-in-time and time-bound rather than as standing admin rights. *(3.1.5)*
- Enforce separation of duties in approval workflows (requester is not the approver). *(3.1.4)*

Endpoint Privilege Management

- Remove local administrator rights from standard users; elevate only specific approved applications. *(3.1.6, 3.1.7)*
- Log every privileged execution and forward the records to the SIEM. *(3.1.7)*

Network Access Control (NAC) + 802.1X / RADIUS

- Authenticate every device to the network via 802.1X before granting access; use certificates where feasible. *(3.1.1, 3.1.16, 3.1.18)*
- Quarantine or deny unknown and non-compliant devices to a remediation VLAN. *(3.1.18)*

Firewalls / Network Segmentation

- Segment the CUI environment (enclave) from the general network with explicit allow rules and a default-deny posture. *(3.1.3, 3.1.20)*

- Enforce information-flow rules between zones with ACLs and VLANs; restrict egress traffic. *(3.1.3)*
- Terminate all remote access through defined, managed firewall/gateway points. *(3.1.14)*

VPN / Remote Access Gateway / ZTNA

- Route 100% of remote access through the managed gateway; do not split-tunnel around the CUI enclave. *(3.1.12, 3.1.14)*
- Use FIPS-validated encryption (IPsec or TLS) for the tunnel. *(3.1.13)*
- Set idle and maximum session timeouts that force re-authentication. *(3.1.11)*
- Require MFA and, for administrative access, route through a bastion / jump host. *(3.1.12, 3.1.15)*

Bastion / Jump Hosts

- Make them the only path to administer CUI systems; block direct admin connections elsewhere. *(3.1.14, 3.1.15)*
- Record sessions and forward all privileged commands to the SIEM. *(3.1.7, 3.1.15)*

SIEM / Centralized Audit Logging

- Aggregate logs from identity, endpoints, PAM, firewalls, and remote-access gateways. *(3.1.7)*
- Alert on privileged-function execution, failed logons, and anomalous remote access. *(3.1.7, 3.1.8, 3.1.12)*

Mobile Device Management / UEM (e.g., Microsoft Intune)

- Enroll and enforce a compliance policy on every device that touches CUI; block non-compliant devices via Conditional Access. *(3.1.18)*
- Enforce full-disk encryption on laptops and mobile devices (BitLocker / FileVault). *(3.1.19)*
- Push session-lock, screen-timeout, and USB / removable-media restrictions. *(3.1.10, 3.1.21)*

Wireless LAN Controller + WPA2 / WPA3-Enterprise

- Require WPA2/WPA3-Enterprise with 802.1X authentication; do not use pre-shared keys for CUI networks. *(3.1.16, 3.1.17)*
- Encrypt all wireless traffic; isolate guest and CUI SSIDs onto separate VLANs. *(3.1.17)*

Data Loss Prevention (DLP)

- Define CUI data classifications and block or alert on unauthorized transfer (email, cloud, removable media). *(3.1.3, 3.1.21, 3.1.22)*
- Restrict copying of CUI to portable storage and to external systems. *(3.1.20, 3.1.21)*

CASB / Secure Web Gateway (Proxy)

- Control and monitor connections to external and cloud systems; allowlist sanctioned services. *(3.1.20)*
- Inspect and filter web/cloud traffic for CUI leakage. *(3.1.3, 3.1.20)*

Endpoint Device Control (USB / Removable Media)

- Default-deny removable storage; permit only encrypted, approved devices where a business need exists. *(3.1.21)*

Web Application Firewall (WAF) + Content-Review Process

- Front public-facing systems with a WAF; enforce a documented review and approval step before content is published. *(3.1.22)*
- Confirm that no CUI is exposed on publicly accessible systems. *(3.1.22)*

Choosing a Compliant Cloud Foundation

Most contractors implement these controls on a FedRAMP-authorized or government-community cloud. Any cloud used to store, process, or transmit CUI must be authorized at the **FedRAMP Moderate** baseline (or demonstrably equivalent); ITAR or export-controlled data raises the bar further.

Microsoft 365 GCC High

The default choice for contractors handling CUI, ITAR, or export-controlled data. A sovereign, US-only environment with US-person support personnel; pairs Entra ID, Intune, Purview, and Defender/Sentinel into a single compliant stack. Highest cost and eligibility bar.

Microsoft 365 GCC (Moderate)

A lower-cost government-community option suited to CUI that is *not* ITAR or export-controlled. Confirm it meets the specific CUI category and flow-down before selecting it, as it is not the sovereign DoD environment.

Microsoft Azure Government

Government-community IaaS/PaaS for custom applications, engineering workloads, and purpose-built CUI enclaves; frequently paired with M365 GCC High for productivity.

AWS GovCloud (US)

An isolated, US-operated AWS region (FedRAMP High authorized) widely used to host product, engineering, and data-processing enclaves that handle CUI. Strong fit for teams already invested in AWS.

Google Workspace & Google Cloud (Assured Workloads / Assured Controls)

Google's controlled configurations support CUI with data-residency and personnel controls. Less common in the DIB today but a viable option for Google-centric organizations.

PreVeil

An end-to-end encrypted email and file-sharing overlay that can dramatically reduce CMMC scope by keeping CUI out of the broader environment. Often used to avoid a full GCC High migration for smaller teams.

Tools for Extracting Structured Configuration Evidence

Wherever possible, capture evidence as **structured, text-based exports** - JSON, XML, CSV, INF, XCCDF, or OSCAL - rather than screenshots. Machine-readable exports are timestamped, show the full setting, and can be ingested directly by a compliance platform.

Microsoft Entra ID / Microsoft 365 (identity, MFA, Conditional Access)

- **Microsoft Graph PowerShell SDK** (`Get-Mg*`) - export users, groups, role assignments, Conditional Access policies, and authentication methods as JSON/CSV. *(3.1.1, 3.1.2, 3.1.5, 3.1.12, 3.1.15)*
- **Microsoft365DSC** - exports the full tenant configuration (Entra, Intune, Purview, Exchange) as declarative, version-controllable text. *(broad AC coverage)*
- **CISA ScubaGear** - automated assessment of M365/Entra secure-configuration baselines, output as JSON plus a readable report. *(3.1.1, 3.1.8, 3.1.12)*

Windows / Active Directory / Group Policy

- **`Get-GPOReport -ReportType Xml`** - every GPO setting, including account lockout, session lock, and logon banners, as XML. *(3.1.8, 3.1.9, 3.1.10)*
- **`secedit /export`** - local security policy to an INF text file; **`gpresult /x`** for resultant set of policy. *(3.1.8, 3.1.10)*
- **`auditpol /get /category:* /r`** - audit policy configuration as CSV. *(3.1.7)*
- **`Get-ADDefaultDomainPasswordPolicy`** and **`Get-BitLockerVolume`** / `manage-bde -status` - lockout and disk-encryption state as JSON/CSV/text. *(3.1.8, 3.1.19)*

Endpoint & Mobile (MDM/UEM, DLP)

- **Microsoft Intune via Graph** - device compliance policies, configuration profiles, and encryption reports as JSON/CSV. *(3.1.10, 3.1.18, 3.1.19, 3.1.21)*
- **Jamf Pro API** (macOS) - configuration profiles and inventory as JSON. *(3.1.18, 3.1.19)*
- **Microsoft Purview** (`Get-DlpCompliancePolicy`) - DLP policy definitions as JSON. *(3.1.3, 3.1.21, 3.1.22)*

Network, Firewall & Wireless

- **Titania Nipper** - parses firewall, router, and switch configs into structured audit findings as XML/CSV/JSON. *(3.1.3, 3.1.14, 3.1.20)*
- **Device-native exports** - `show running-config` (Cisco), the XML API export (Palo Alto), or config backup (Fortinet) as text/XML. *(3.1.3, 3.1.14)*
- **Oxidized / RANCID** - automated network-config backup to text under version control. *(3.1.14)*
- **Wireless controller exports** (Cisco WLC, Aruba) - WPA2/WPA3-Enterprise and 802.1X settings as text. *(3.1.16, 3.1.17)*

Cloud Posture (Azure, AWS, GCP)

- **Azure CLI** (`az ... -o json`) and **Microsoft Defender for Cloud** - includes a built-in NIST SP 800-171 regulatory-compliance report you can export. *(broad)*
- **AWS CLI** (`aws iam get-account-authorization-details`) and **AWS Config** - account, IAM, and resource configuration as JSON. *(3.1.1, 3.1.2, 3.1.20)*
- **Prowler / ScoutSuite / Steampipe** - multi-cloud CIS/NIST configuration checks as JSON/CSV/HTML. *(broad)*

SCAP & Benchmark Scanners (authoritative, structured)

- **DISA SCAP Compliance Checker (SCC)** with STIG benchmarks - results as XCCDF/OVAL/ARF XML. *(broad, host-level)*
- **OpenSCAP** (`oscap`) for Linux hosts - XCCDF/ARF XML results. *(broad, host-level)*
- **Microsoft Security Compliance Toolkit / PolicyAnalyzer** - baseline comparisons exportable to XML/CSV. *(3.1.8, 3.1.10)*

OSCAL & Compliance Automation (the structured-format endgame)

- **OSCAL** (NIST Open Security Controls Assessment Language) - represent your SSP, components, and assessment results as JSON/XML/YAML. *(all AC)*
- **IBM compliance-trestle (Trestle)** - author and validate OSCAL artifacts programmatically. *(all AC)*

Practical tip: for every export, record what was run, on which system, and when. A traceable, dated artifact is worth far more than an undated screenshot.

Conclusion

The Access Control family rewards a design-first approach. Anchor the environment on a strong identity provider, enforce MFA and least privilege everywhere, segment a well-defined CUI enclave, and centralize logging - and the majority of the family falls into place.

The July 2026 suspension of CMMC Phase 2 paused the third-party certification milestone, not the underlying obligation: NIST SP 800-171, DFARS 252.204-7012, and the Level 2 self-assessment remain fully in force. Implementing this family well is still required today.

Glossary of Acronyms

ACL	Access Control List
ARF	Asset Reporting Format (SCAP results format)
BYOD	Bring Your Own Device
C3PAO	CMMC Third-Party Assessor Organization
CASB	Cloud Access Security Broker
CMMC	Cybersecurity Maturity Model Certification
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DLP	Data Loss Prevention
FCI	Federal Contract Information
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
GCC	Government Community Cloud
GPO	Group Policy Object
IdP	Identity Provider
ITAR	International Traffic in Arms Regulations
MDM / UEM	Mobile Device Management / Unified Endpoint Management
MFA	Multi-Factor Authentication
NAC	Network Access Control

NIST	National Institute of Standards and Technology
OSCAL	Open Security Controls Assessment Language
PAM	Privileged Access Management
POA&M	Plan of Action and Milestones
RBAC	Role-Based Access Control
SCAP	Security Content Automation Protocol
SIEM	Security Information and Event Management
SPRS	Supplier Performance Risk System
SSP	System Security Plan
STIG	Security Technical Implementation Guide
VPN	Virtual Private Network
WAF	Web Application Firewall
XCCDF	Extensible Configuration Checklist Description Format
ZTNA	Zero Trust Network Access

About Methodical Security

Methodical Security provides resources and tooling to support Defense Industrial Base organizations through CMMC / NIST SP 800-171 assessments. Its platform, **Certalo**, works at the determination-statement level: it maps your existing documentation to each objective, flags where evidence is thin, and compresses the path to a submission-ready SSP, Assessment Report, and SPRS package. The result turns a one-time compliance scramble into a repeatable process — protecting current revenue and opening new contract eligibility.