COMPLIANCE ALIGNMENT GUIDE

Total Access Control (TAC) and CMMC 2.0

How TAC delivers the access control, authentication, and audit requirements at the heart of CMMC 2.0 Level 2 — the NIST SP 800-171 control families that gate Defense Industrial Base contracts.

Audience	Framework	Version
DIB contractors & subcontractors, CISOs, CMMC / 800-171 compliance leads	CMMC 2.0 Level 2 (NIST SP 800-171)	v1.0 — 2026

TAC Scope in CMMC 2.0. CMMC 2.0 Level 2 maps one-to-one to the 110 security requirements of NIST SP 800-171, organized into 14 control families. TAC delivers the technical controls in the families concerned with electronic access to Controlled Unclassified Information (CUI): **Access Control (AC), Identification & Authentication (IA), and Audit & Accountability (AU)**, with supporting coverage for System & Communications Protection (SC).

Achieving CMMC Level 2 requires implementing all 14 control families and passing a C3PAO assessment (or authorized self-assessment). TAC is one technical component of that effort; it does **not**, by itself, make an organization CMMC certified, nor does it address the administrative, physical, personnel, training, or program-governance families, the System Security Plan, or the Plan of Action & Milestones.

Overview

The Cybersecurity Maturity Model Certification (CMMC) 2.0 exists to verify that the Defense Industrial Base protects Controlled Unclassified Information. Its three levels build on a single foundation: Level 1 covers basic safeguarding of Federal Contract Information; Level 2 maps directly to the 110 security requirements of NIST SP 800-171 across 14 control families; Level 3 adds enhanced controls from NIST SP 800-172.

The relationship is simple: NIST 800-171 provides the “what” — the requirements for protecting CUI — and CMMC provides the “how” — the verification, through self-assessment or third-party (C3PAO) certification, depending on the contract. With the DFARS CMMC final rule now in effect, CMMC language is appearing in new DoD contracts, and certification is increasingly a prerequisite to bid or retain defense work. Several of the most heavily weighted families — Access Control (the largest technical domain), Identification & Authentication, and Audit & Accountability — are fundamentally access control problems, which is exactly where TAC delivers.

DOMAIN AC — 800-171 §3.1 — PRIMARY COVERAGE

Access Control

CMMC REQUIREMENT	HOW TAC DELIVERS
Limit access to authorized users (3.1.1, 3.1.2)	Access to CUI systems is limited to authorized users, processes, and devices, and to the specific transactions each is permitted. TAC enforces this per-user, per-application, on every request at the reverse proxy.
Least privilege (3.1.5)	Users receive only the access their role requires. Privileged access is separately scoped with stronger policy. Users see only the CUI resources they are authorized to reach.
Control remote access (3.1.12–3.1.14)	All remote access to CUI is brokered and monitored through TAC, routed through a single encrypted port, and permitted only via the managed access control point. No direct, unmediated remote paths to CUI systems remain.
Control mobile device connection (3.1.18)	Mobile and remote devices are subject to posture validation before access to CUI is granted, and continuously thereafter. Non-compliant devices are denied without an endpoint agent requirement.
Limit unsuccessful logon attempts (3.1.8)	Failed authentication attempts are rate-limited and logged at the proxy, with configurable lockout to prevent brute-force attacks against CUI systems.

DOMAIN IA — 800-171 §3.5 — PRIMARY COVERAGE

Identification & Authentication

CMMC REQUIREMENT	HOW TAC DELIVERS
Identify users, processes, devices (3.5.1)	Every user, service account, AI agent, and device is uniquely identified and authenticated before reaching CUI. TAC federates with Active Directory, LDAP, SAML, OIDC, RADIUS, and SQL identity sources.
Multifactor authentication (3.5.3)	MFA is enforced for local and network access to privileged accounts and for network access to non-privileged accounts. All seven methods are included in the base licence: FIDO2/WebAuthn, SafeLogin, TOTP, push, SMS, OTP, and hardware tokens, plus Duo, RSA, and biometric integration.
Replay-resistant authentication (3.5.4)	Phishing-resistant FIDO2/WebAuthn and session-scoped tokens provide replay-resistant authentication mechanisms for network access to CUI.
Authenticator management (3.5.7–3.5.10)	TAC enforces MFA regardless of upstream password strength. Authenticator lifecycle remains in the organization’s identity source of truth; TAC stores no portable credentials and issues session-scoped tokens only.

DOMAIN AU — 800-171 §3.3 — PRIMARY COVERAGE

Audit & Accountability

CMMC REQUIREMENT	HOW TAC DELIVERS
Create & retain audit logs (3.3.1)	Every authentication, authorization decision, session, and policy event involving CUI access is logged with full attribution, enabling the monitoring, analysis, investigation, and reporting of unlawful or unauthorized activity.
Trace actions to individual users (3.3.2)	Because every session ties to a uniquely authenticated identity, every logged access action is traceable to a specific individual — satisfying the individual-accountability requirement.
Audit content & time stamps (3.3.7)	Logs capture identity, source, target system, action, and time-stamped result of every access event, providing the audit-record content CMMC requires.
SIEM export for review (3.3.3–3.3.6)	TAC logs export to SIEM for the review, analysis, reporting, and reduction CMMC requires. TAC provides the access-event evidence assessors expect to see operating.

DOMAIN SC — 800-171 §3.13 — SUPPORTING COVERAGE

System & Communications Protection

CMMC REQUIREMENT	HOW TAC DELIVERS
Protect communications confidentiality (3.13.8, 3.13.11)	All access to CUI through TAC is encrypted in transit (TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules), protecting CUI on the access path. CUI confidentiality at rest is an application/storage-layer responsibility.
Boundary protection & managed access points (3.13.1, 3.13.5)	TAC's single-port reverse proxy is the managed boundary in front of CUI systems. All other inbound ports close, monitoring and controlling communications at the external boundary and key internal boundaries.
Deny by default (3.13.6)	Network traffic to CUI systems is denied by default and permitted only by explicit policy exception at the proxy — the deny-all, permit-by-exception posture CMMC expects.

Out of Scope — the remaining control families and the certification itself. CMMC 2.0 Level 2 requires all 14 NIST 800-171 control families. TAC does not address Awareness & Training, Configuration Management (beyond access-related boundary configuration), Incident Response, Maintenance, Media Protection, Personnel Security, Physical Protection, Risk Assessment, or Security Assessment — these are administrative, physical, personnel, and program activities outside the scope of an access control platform. TAC also does not produce the System Security Plan (SSP) or Plan of Action & Milestones (POA&M), and it cannot make an organization "CMMC certified" — Level 2 certification is granted only through a C3PAO assessment or an authorized self-assessment of the complete program. TAC produces the technical access, authentication, and audit evidence assessors expect for the AC, IA, and AU families, of which it is one component.

One Platform Across CMMC, NIST, and FedRAMP

Because CMMC 2.0 Level 2 is a direct adoption of NIST SP 800-171 — itself a refined subset of NIST 800-53 — the access controls that satisfy CMMC are the same ones that satisfy NIST and FedRAMP. The MFA enforcement that meets CMMC IA controls meets NIST IA controls. The audit logging that meets CMMC AU controls meets NIST AU controls. The boundary protection that meets CMMC SC controls meets FedRAMP boundary requirements.

For a defense contractor, this means the access-control evidence is built once and reused across every framework a contract may require. You are not standing up a separate CMMC access program — you are applying one platform to all of them, then pointing your C3PAO assessor at the same logs, the same authentication records, and the same enforcement policies.

Control Family Coverage Summary

CMMC / 800-171 FAMILY	WHAT TAC ADDRESSES	TAC COVERAGE
AC — Access Control	Authorized-user limits, least privilege, remote/mobile access, logon controls	Primary
IA — Identification & Auth	Unique ID, MFA, replay-resistant auth, authenticator management	Primary
AU — Audit & Accountability	Access logging, individual traceability, audit content, SIEM export	Primary
SC — System & Comms Protection	Encryption in transit, boundary protection, deny-by-default	Supporting
AT / CM / IR / MA / MP / PS / PE / RA / CA	Training, incident response, physical, personnel, risk & program controls	Out of scope
Certification process	SSP, POA&M, C3PAO assessment / self-assessment	Out of scope

Next Steps

Map your CUI access architecture against the CMMC Level 2 control families. Identify the AC, IA, and AU requirements TAC satisfies for your CUI systems and the evidence your assessor will expect. **Request a CMMC walkthrough** at portsys.com/contact or info@portsys.com — a PortSys specialist will work through your environment and produce a prioritised plan with the access-evidence package your C3PAO assessment will require.