COMPLIANCE ALIGNMENT GUIDE

Total Access Control (TAC) and NIST

How TAC maps to NIST SP 800-207 (Zero Trust Architecture), NIST SP 800-171 (Protecting Controlled Unclassified Information), and the NIST Cybersecurity Framework — for federal agencies, defense industrial base contractors, and CMMC 2.0 candidates.

Audience	Frameworks	Version
Federal & DoD CISOs, CUI handlers, DIB contractors, CMMC 2.0 candidates	NIST SP 800-207, SP 800-171, NIST CSF	v2.0 — 2026

Overview

The National Institute of Standards and Technology (NIST) publishes three frameworks critical to federal cybersecurity programs: **NIST SP 800-207** defines the federal standard for Zero Trust Architecture; **NIST SP 800-171** protects Controlled Unclassified Information (CUI) and underpins CMMC 2.0 compliance for defense industrial base contractors; and the **NIST Cybersecurity Framework** provides the foundational protect-detect-respond-recover model adopted across sectors.

Total Access Control (TAC) by PortSys is a purpose-built zero-trust access control platform that **implements the Policy Engine, Policy Administrator, and Policy Enforcement Point** defined in NIST SP 800-207 within a single, unified platform — while addressing specific 800-171 control families and key NIST CSF Protect outcomes for the applications and systems it fronts.

> **TAC Scope in NIST.** TAC controls **access to applications and systems handling CUI** — administrative consoles, operations tools, federal portals, dashboards, and other applications. TAC addresses access control, authentication, audit, boundary protection, and communications encryption requirements (800-171 Families 3.1, 3.3, 3.5, 3.13) for systems in scope, and implements all seven 800-207 zero trust tenets.
>
> TAC does **not** encrypt CUI at rest, scan or sanitise CUI content, replace network segmentation between enclaves, or perform vulnerability scanning. Families such as 3.7 (Maintenance), 3.8 (Media Protection), 3.9 (Personnel Security), 3.10 (Physical Protection), 3.11 (Risk Assessment), and 3.12 (Security Assessment) are satisfied by complementary controls in your environment.

Part A: NIST SP 800-207 — Zero Trust Architecture

NIST SP 800-207 defines Zero Trust Architecture through three logical components: the **Policy Engine (PE)** makes access decisions, the **Policy Administrator (PA)** communicates them and manages sessions, and the **Policy Enforcement Point (PEP)** enforces them at the point of access. TAC implements all three components in a single platform, eliminating the integration complexity of multi-vendor zero trust architectures.

ZT TENETS

The Seven Tenets of NIST SP 800-207

REQUIREMENT	HOW TAC DELIVERS
Tenet 1 — All data sources and computing services are considered resources	TAC treats every application — web, thick-client, forms-based, Kerberos, IoT, API, and AI agent endpoint — as a protected resource. No application type is excluded from zero-trust enforcement.
Tenet 2 — All communication is secured regardless of network location	TAC's reverse-proxy architecture enforces identical security policies for all users regardless of whether they are on-premises, remote, or on partner networks. All traffic is encrypted via TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules through a single port. Network location never confers trust.
Tenet 3 — Access granted on a per-session basis	Per-request policy evaluation ensures that access is never permanently granted. Each request is independently evaluated against current identity, device posture, geolocation, and policy. Mid-session revocation is supported if device compliance or policy conditions change.
Tenet 4 — Access determined by dynamic policy	TAC's unified policy engine evaluates access based on identity attributes, device posture, geolocation, time of day, and application sensitivity. Policies are centrally managed and dynamically enforced. (Note: TAC uses configurable rules, not ML-based behavioural anomaly detection — external threat intelligence and risk signals can be ingested via API or syslog to inform policy.)
Tenet 5 — Monitor security posture of all owned and associated assets	Continuous device posture validation checks OS version, patch level, antivirus status, disk encryption, firewall status, and domain membership on every request. Non-compliant devices are denied access or required to remediate. Service accounts and AI agents are monitored under the same policy framework.
Tenet 6 — Authentication and authorisation are dynamic and strictly enforced before access	Authentication via multi-factor methods (built-in FIDO2 / WebAuthn, SafeLogin proprietary, TOTP, push, SMS, OTP, hardware tokens; plus third-party integration with Duo, RSA, Swivel, biometric solutions, and others) and authorisation via policy engine occur before every access decision. No implicit trust based on prior authentication.
Tenet 7 — Collect information about asset state and use it to improve security posture	Comprehensive audit logging captures every access request with full context: user identity, authentication method, device posture, source IP, geolocation, timestamp, application accessed, policy decision, and session duration. Native real-time monitoring and alerting; optional SIEM export via syslog or API for downstream correlation and forensic analysis.

DEPLOYMENT MODEL

TAC and 800-207 Section 3.2.1 (Resource-Portal Model)

REQUIREMENT	HOW TAC DELIVERS
Unified PE + PA + PEP architecture	TAC implements the Policy Engine, Policy Administrator, and Policy Enforcement Point in one platform. This eliminates the policy synchronisation challenges common in multi-vendor zero trust deployments — decisions, communication, and enforcement happen in the same engine.
Resource-Portal model alignment	TAC aligns with the resource-portal deployment model described in 800-207 Section 3.2.1: a gateway-based reverse proxy that mediates access between subjects and enterprise resources. Applications behind TAC are never directly addressable from any network.
Single-tenant deployment flexibility	Every TAC deployment is a dedicated Secure Virtual Appliance — on-premises in government facilities, in FedRAMP-authorised cloud regions (AWS GovCloud, Azure Government), in commercial cloud accounts, or in air-gapped environments. The customer controls the infrastructure; TAC adapts to the deployment model.

Part B: NIST Cybersecurity Framework — Protect (PR.AC)

The NIST Cybersecurity Framework's Protect function includes Identity Management and Access Control (PR.AC), a category where TAC directly addresses multiple outcomes for the applications it fronts.

CSF PROTECT

Identity Management & Access Control (PR.AC)

REQUIREMENT	HOW TAC DELIVERS
PR.AC-1 — Identities and credentials managed	TAC identity federation manages credential validation across all connected directory sources (Active Directory, LDAP, SAML, RADIUS, OIDC, SQL, custom). Real-time revocation when user status changes in the source directory.
PR.AC-3 — Remote access managed	TAC reverse proxy provides authenticated, policy-governed remote access to all protected applications without exposing network ports. Can replace traditional VPN for application access while maintaining per-application policy, MFA, device posture, and full audit trail.
PR.AC-4 — Access permissions and authorisations managed	Unified policy engine manages access rights across all identity sources with granular per-application, per-user policies. Role-based and attribute-based access control supported. Policy changes take effect immediately.
PR.AC-5 — Network integrity protected	All access flows through a single encrypted channel (TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules). TAC is the sole gateway to protected applications. Other inbound ports closed at the firewall.

REQUIREMENT	HOW TAC DELIVERS
PR.AC-7 — Users, devices, and other assets authenticated commensurate with risk	Risk-appropriate authentication through layered factors: identity verification, MFA, device posture, geolocation, and time-of-day rules. Step-up authentication configurable per application based on sensitivity.

Part C: NIST SP 800-171 — Protecting CUI

NIST SP 800-171 establishes the security requirements for protecting Controlled Unclassified Information (CUI) in non-federal systems. It is the foundation of CMMC 2.0 compliance for defense industrial base contractors.

AC FAMILY

Access Control (3.1)

REQUIREMENT	HOW TAC DELIVERS
3.1.1 — Limit system access to authorised users	TAC identity federation connects to all major directory services. Only authenticated users matching access policy reach applications handling CUI.
3.1.2 — Limit system access to authorised functions	Policy engine restricts each user to only the applications and functions they are explicitly permitted to access. Per-application authorisation enforced on every request.
3.1.3 — Control CUI flow	TAC mediates and logs all access paths to applications containing CUI. (Note: TAC controls access to CUI-containing applications, not information flow within applications. Data-level CUI flow controls require complementary DLP or application-layer controls.)
3.1.5 — Employ principle of least privilege	Granular policy engine grants minimum required access per user, per application, per session. No standing administrative access; privilege elevation requires explicit policy match.
3.1.12 — Monitor and control remote access sessions	Every remote session is authenticated, device-posture-validated, policy-governed, and fully logged. Real-time session revocation supported — policy changes take effect immediately.
3.1.13 — Employ cryptographic mechanisms to protect remote access	All remote access traffic encrypted via TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules. Single encrypted port for all communications.
3.1.20 — Verify external connections	All external connections pass through TAC's identity verification, MFA, device posture, and policy evaluation before reaching protected applications. No anonymous or unverified external access path exists.

IA FAMILY

Identification and Authentication (3.5)

REQUIREMENT	HOW TAC DELIVERS
3.5.1 — Identify system users, processes, and devices	Every user, service account, AI agent, and device identified against connected identity sources before any access is granted. The same policy engine governs human and non-human identities. Critical for federal environments deploying AI workloads against CUI.
3.5.2 — Authenticate user, process, and device identities	Identity verification required for every user, process, and device before access. Built-in MFA includes FIDO2 / WebAuthn (phishing-resistant), SafeLogin (proprietary), TOTP, push notifications, SMS, OTP, and hardware tokens. Third-party MFA integration with virtually any provider including Duo, RSA, Swivel, biometric solutions, and others. All MFA methods included in base licence.
3.5.3 — Use MFA for privileged and non-privileged accounts	MFA mandatory for all access to CUI applications, including legacy applications that cannot natively support modern authentication. MFA applies to both privileged administrative access and standard user access.
3.5.6 — Disable identifiers after inactivity	Session timeout policies are configurable per application and user group. Real-time access revocation when user status changes in the source directory — no need to wait for next login cycle.

AU FAMILY

Audit and Accountability (3.3)

REQUIREMENT	HOW TAC DELIVERS
3.3.1 — Create and retain system audit records	Comprehensive audit log of every access event — user identity, authentication method, device posture, source IP, geolocation, timestamp, application accessed, and policy decision. Logging is automatic and cannot be disabled for protected applications.
3.3.2 — Ensure user actions are uniquely traceable	Every action attributed to a verified identity. No anonymous or pseudonymous access to CUI applications. Service accounts and AI agents are uniquely identified.
3.3.4 — Alert on audit logging process failure	TAC provides native real-time monitoring and alerting on access events and platform health. Logging failures or platform issues are surfaced through the admin console and via SIEM integration.
3.3.6 / 3.3.7 — Audit reduction and time stamps	Centralised audit data exportable via syslog or API to your SIEM for downstream correlation, reduction, and reporting. All log entries include authoritative timestamps.
3.3.8 — Protect audit information	Tamper-evident, centralised logging. Audit data cannot be modified through the TAC console. Export controls preserve integrity for downstream forensic analysis.

REQUIREMENT	HOW TAC DELIVERS
3.3.9 — Limit management of audit logging functionality	Audit logging configuration is restricted to authorised administrators through TAC's admin policy framework. Administrative actions on the audit logging functionality are themselves logged.

SC FAMILY

System and Communications Protection (3.13)

Scope note. TAC addresses boundary protection and cryptographic protection in transit. TAC does *not* address protection of CUI at rest (3.13.11, 3.13.16), denial-of-service protection (3.13.6), or collaborative computing device controls (3.13.12). Those controls require complementary infrastructure and endpoint controls in your environment.

REQUIREMENT	HOW TAC DELIVERS
3.13.1 — Monitor, control, and protect communications at external boundaries	TAC's reverse-proxy architecture is the external boundary for protected applications. All inbound traffic monitored, controlled by policy, and protected by encryption. Other inbound ports closed at the firewall.
3.13.5 — Implement subnetworks for publicly accessible system components	TAC enforces a logical separation between public-facing access (the TAC entry point) and the trusted application zone. CUI applications are never directly addressable from the internet; the TAC proxy is the sole intermediary.
3.13.8 — Implement cryptographic mechanisms to prevent unauthorised disclosure during transmission	All traffic to and from protected applications encrypted via TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules. Single encrypted port for all access. End-to-end encryption between the user's device and TAC, and between TAC and the backend application.
3.13.15 — Protect authenticity of communications sessions	Every connection is authenticated and policy-evaluated. Sessions cannot be hijacked through network-level attacks because the encrypted channel terminates at the TAC proxy with strong session controls. Mid-session device posture changes trigger immediate session revocation.

Why TAC Is Uniquely Strong for NIST

Unified PE + PA + PEP — One Platform. NIST 800-207 defines three logical zero trust components: Policy Engine, Policy Administrator, and Policy Enforcement Point. TAC implements all three in a single, integrated platform. No multi-vendor integration. No policy synchronisation drift. No gaps between components — decisions, communication, and enforcement happen in the same engine.

Close All Ports — Minimum Attack Surface for CUI. TAC closes all inbound firewall ports except one encrypted channel (TLS 1.2 or TLS 1.3 with FIPS 140-2 modules) for the CUI applications it fronts. Most competing approaches leave datacenter ports open behind their cloud or concentrator — TAC closes them. Critical for federal authorisations where attack surface is heavily scrutinised.

Legacy Federal Application Protection. Many federal agencies and DIB contractors run critical CUI systems on legacy applications that cannot natively support MFA or modern authentication. TAC injects MFA, device posture,

and continuous validation in front of any application — without changing a single line of code or requiring re-authorisation.

Single-Tenant Isolation — Sovereign CUI Boundaries. Every TAC deployment is a dedicated, isolated Secure Virtual Appliance — on-premises, in FedRAMP-authorised cloud regions, in your cloud account, or in air-gapped environments. Policies and audit data for your CUI never co-mingle with another organisation's environment. Matters for federal customers with sovereignty or compartmentalisation requirements.

All-Inclusive Licensing — No Authorisation Gaps. TAC includes every security feature in the base licence: all MFA methods, device posture validation, AI agent governance, SSO, and 24×7 support. No add-on tiers, no per-user MFA surcharges. Eliminates the risk of authorisation gaps caused by deferred security purchases.

NIST Coverage Summary

CONTROL FAMILY / FRAMEWORK	CONTROLS ADDRESSED	TAC COVERAGE
NIST SP 800-207	Zero Trust Architecture (PE / PA / PEP)	All three logical ZTA components in one platform; all 7 ZT tenets addressed end-to-end
NIST CSF — Protect	Identity Management & Access Control (PR.AC)	Identity management, remote access, network integrity, risk-appropriate authentication
NIST 800-171 — 3.1	Access Control	Authorised access, least privilege, CUI access mediation, remote sessions, FIPS 140-2 encryption
NIST 800-171 — 3.3	Audit and Accountability	Comprehensive attributed audit trail, tamper-evident logging, native real-time alerting, SIEM export
NIST 800-171 — 3.5	Identification and Authentication	Multi-directory federation, built-in & third-party MFA, service accounts & AI agents, device posture
NIST 800-171 — 3.13	System and Communications Protection (partial)	Boundary protection, public-access boundary, TLS 1.2/1.3 with FIPS 140-2; does not address CUI at rest

Next Steps

Map your CUI application inventory. Identify every administrative console, operations tool, portal, dashboard, and integration that handles CUI — each is a candidate for TAC mediation. **Request a NIST compliance walkthrough** at portsys.com/contact or info@portsys.com — a PortSys specialist will walk through your specific environment, identify high-priority CUI applications, and produce a prioritised deployment plan with timeline and milestones.

© 2026 PortSys, Inc. All rights reserved.
Maps TAC capabilities to NIST SP 800-207, SP 800-171, and the NIST CSF. Compliance is determined by authorised assessors against the complete organisational security programme. TAC is one component — PortSys recommends working with qualified NIST/CMMC advisors.