COMPLIANCE ALIGNMENT GUIDE

Total Access Control (TAC) and the FBI CJIS Security Policy

How TAC delivers the access control, advanced authentication, and audit requirements of the FBI CJIS Security Policy v6.0 — for the agencies and contractors that access Criminal Justice Information.

Audience	Framework	Version
Law enforcement & criminal justice agencies, CJI contractors, state CSAs, IT security leads	FBI CJIS Security Policy v6.0	v1.0 — 2026

TAC Scope in CJIS. The FBI CJIS Security Policy v6.0 organizes requirements into 20 policy areas mapped to NIST 800-53 controls. TAC delivers the technical controls in the policy areas concerned with electronic access to Criminal Justice Information (CJI): **Access Control (5.5), Identification & Authentication (5.6), and Audit & Accountability (5.4)**, with supporting coverage for configuration and system communications (5.7, 5.10).

Full CJIS compliance requires an end-to-end program including personnel screening, security awareness training, physical and environmental protection, media protection, incident response, and formal governance — activities outside the scope of any access control platform. TAC addresses the electronic access, authentication, and audit layer; not the personnel, physical, training, or program-governance layers.

Overview

The CJIS Security Policy exists to protect Criminal Justice Information — biometrics, case records, and identifiable data about individuals — from unauthorized access. Several of its most heavily audited policy areas are, at their core, access control problems: who can reach CJI, how they prove their identity, and whether every access is logged.

Advanced authentication — multi-factor authentication for privileged and non-privileged accounts — became mandatory and subject to FBI audit as of October 1, 2024. Version 6.0 reinforces stronger identity proofing, MFA, account lifecycle management, rapid account disabling, and expanded audit and evidence expectations. Because v6.0 is mapped to NIST 800-53, agencies already aligned with NIST or FedRAMP are well positioned — and so is any access platform built on those same controls. The CJIS Security Policy is architecture-independent, and so is TAC: it protects CJI access whether systems run on-premises, in the cloud, or hybrid.

POLICY AREA 5.5 — PRIMARY COVERAGE

Access Control

CJIS REQUIREMENT	HOW TAC DELIVERS
Account management	Access to CJI-bearing systems is governed through the agency's identity source, which TAC consumes. Individual accountability is enforced — every session ties to a verified individual identity. No shared accounts are required.
Least privilege & access enforcement	Per-user, per-application policy is enforced at the proxy on every request. Users reach only the CJI systems their role authorizes — nothing else is visible or reachable.
Rapid account disabling	Disabling a user at the identity source immediately revokes their TAC sessions and blocks future access to all CJI systems at once — meeting v6.0's emphasis on rapid account disabling when risk is detected.
Remote & mobile access control	Remote and mobile access to CJI is brokered through TAC on a single encrypted port, with device posture validated before access is granted. No open inbound ports to CJI systems remain.

POLICY AREA 5.6 — PRIMARY COVERAGE

Identification & Authentication

CJIS REQUIREMENT	HOW TAC DELIVERS
Advanced authentication (MFA)	MFA is enforced on every session for both privileged and 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 — satisfying the advanced authentication mandate auditable since October 1, 2024.
Unique identification	Every user and entity is uniquely identified and authenticated before reaching CJI. TAC federates with the agency's Active Directory, LDAP, SAML, OIDC, or other identity source.
Authenticator management	TAC enforces MFA regardless of upstream password strength. Authenticator lifecycle remains in the agency's identity source of truth; TAC issues session-scoped tokens with no portability outside the proxy.
Device posture before access	TAC validates device posture — certificate, OS, patch level, encryption, and more — before granting access to CJI systems, and continuously throughout the session.

POLICY AREA 5.4 — PRIMARY COVERAGE

Audit & Accountability

CJIS REQUIREMENT	HOW TAC DELIVERS
Event logging	Every authentication, authorization decision, session establishment, and policy event involving CJI access is logged with full attribution — who accessed what, when, from which device, under what policy.
Audit record content & time stamps	Logs capture the identity, source, target system, action, and time-stamped result of every access event, meeting v6.0's expanded content-of-audit-records requirements.
SIEM export & retention	TAC logs export to SIEM for the retention, review, analysis, and reporting CJIS requires. The agency demonstrates — not just asserts — that CJI access controls are operating, with TAC providing the access evidence.

POLICY AREAS 5.7 & 5.10 — SUPPORTING COVERAGE

Configuration & System Communications

CJIS REQUIREMENT	HOW TAC DELIVERS
Encryption in transit	All access to CJI through TAC is encrypted (TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules), meeting CJIS encryption-in-transit requirements for CJI.
Boundary protection	TAC's single-port reverse proxy is the controlled boundary in front of CJI systems. All other inbound ports close, reducing the attack surface CJIS configuration controls aim to minimize.

Out of Scope — Personnel, physical, training, media, incident response & governance policy areas. The CJIS Security Policy includes policy areas TAC does not address: personnel security and screening, security awareness training, physical and environmental protection, media protection and sanitization, the formal incident response program, mobile device management beyond access enforcement, and the overarching governance, risk-management, and audit-readiness program v6.0 emphasizes. These are personnel, physical, procedural, and organizational activities outside the scope of an access control platform. TAC produces audit evidence (access logs, authentication records, revocation timelines) that supports the recordkeeping and accountability expectations across several of these areas, but it does not perform the personnel, physical, training, or program-governance functions themselves.

Built on NIST 800-53 — the Same Foundation You Already Align To

CJIS Security Policy v6.0 is mapped to NIST 800-53, and the FBI explicitly notes that agencies already aligned with NIST or FedRAMP are positioned to meet CJIS faster. TAC is built on those same controls. The access enforcement, MFA, device posture, and audit logging that satisfy the CJIS Access Control, Identification & Authentication, and Audit & Accountability policy areas are the same capabilities TAC brings to NIST 800-53 and FedRAMP alignment.

For an agency or contractor handling CJI, this means the access evidence is shared across frameworks. The audit log that demonstrates CJIS event logging is the same one that supports NIST AU controls. The MFA enforcement that satisfies CJIS advanced authentication is the same that satisfies NIST IA controls. You are not building a separate access-control program for CJIS — you are applying one platform to all of them.

CJIS Policy Area Coverage Summary

CJIS POLICY AREA	WHAT TAC ADDRESSES	TAC COVERAGE
5.5 Access Control	Account management, least privilege, rapid disabling, remote/mobile access	Primary
5.6 Identification & Auth	MFA (advanced auth mandate), unique ID, authenticator mgmt, device posture	Primary
5.4 Audit & Accountability	Event logging, audit record content, SIEM export & retention	Primary
5.7 / 5.10 Config & Comms	Encryption in transit, boundary protection	Supporting
Personnel / Physical / Training / Media / IR / Governance	Not addressed — program, personnel & physical activities	Out of scope

Next Steps

Map your CJI access architecture against the CJIS Security Policy v6.0. Identify the Access Control, Identification & Authentication, and Audit & Accountability requirements TAC satisfies for your CJI systems. **Request a CJIS 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 CJIS audit will expect.