NuHarbor SECURITY

CJIS Compliance Requirements: The 2026 Checklist for State & Local Agencies

CJIS Compliance Requirements: The 2026 Checklist for State & Local Agencies

Criminal Justice Information (CJI) is mission-critical. The FBI's CJIS Security Policy v6.0 (Dec 27, 2024) is the current baseline for how state, local, and higher-ed public safety programs must protect that data—regardless of whether systems run on-prem, in the cloud, or hybrid. Version 6.0 reinforces that the policy is architecture-independent and explicitly empowers agencies to tune implementations to risk while still meeting the common baseline.

Changes in 6.0 at a glance

- **Modernized front-matter & governance.** Executive Summary; Sections 1–3 (Approach, Roles & Responsibilities) refreshed to reflect current program reality.
- **Authenticator guidance clarified.** v6.0 spells out which authenticator types must change annually and the use of a "banned password" list.
- **Four families substantially updated: SA** (System & Services Acquisition); **SR** (Supply-Chain Risk Management); **PS** (Personnel Security); **CA** (Assessment, Authorization & Continuous Monitoring).
- **Appendices J & K removed.** (Other guidance appendices remain, including best practices for virtualization, VoIP, cloud, mobile, encryption, IR, and secure coding.)
- **Priority tags introduced.** Controls carry P1–P4 markers to help sequence implementation (examples shown in the family lists below).

IEA – Information Exchange Agreements

- ☐ **Do now:** Inventory every CJI data flow and place a signed agreement (with CJIS Security Addendum where required) on each exchange.
- ☐ **Operate:** Maintain a current data-flow diagram and annually verify encryption, access, and logging match the agreement terms.
- ☐ **Prove it:** Produce the signed agreements, the system-level data-flow map, and an interface control checklist per connection.

Common gaps: Shadow SFTP/API paths, stale agreements after vendor swaps, and unlogged partner endpoints.

AC – Access Control

- ☐ **Do now:** Enforce least-privilege RBAC, separate admin from user identities, and run quarterly access reviews.
- ☐ **Operate:** Require session timeouts, re-auth for sensitive actions, and controlled break-glass access with post-use review.
- ☐ **Prove it:** Show a role catalog, review attestations, and a user-to-rights trace for sample accounts.

Common gaps: Zombie accounts after transfers, shared admin credentials, and over-privileged service accounts.

IA - Identification & Authentication

- ☐ **Do now:** Enable MFA for all users touching CJI and adopt a banned-password list with documented exceptions.
- ☐ **Operate:** Use replay-resistant authenticators, require device unlock plus MFA for direct CJI access, and rotate authenticators on schedule.
- ☐ **Prove it:** Provide MFA policy, IdP configuration evidence, success/failure logs, and an exception register.

Common gaps: Legacy portals without MFA, weak OTP delivery paths, and inconsistent enforcement on mobile/VPN.

AT - Awareness & Training

- ☐ **Do now:** Deliver annual, role-based CJIS security training to everyone who creates, stores, transmits, or accesses CJI.
- ☐ **Operate:** Add phishing simulations and tabletop injects and tie training completion to access enablement.
- ☐ **Prove it:** Export completion rosters, curricula, and quiz or exercise results from the LMS.

Common gaps: Contractors missing from the LMS and accounts left active despite lapsed training.

AU - Auditing & Accountability

- ☐ **Do now:** Define auditable events, centralize logs with time sync, and retain them per policy.
- ☐ **Operate:** Alert on anomalies, route high-risk events to IR, and protect log integrity and retention.
- ☐ **Prove it:** Show SIEM queries, retention settings, and end-to-end event trails for sample incidents.

Common gaps: Uncollected cloud/provider logs, missing admin activity auditing, and unsynchronized clocks.

CA — Assessment, Authorization & Continuous Monitoring

- ☐ **Do now:** Keep a living SSP, run control assessments, track gaps in a POA&M, and stand up continuous monitoring.
- ☐ **Operate:** Automate evidence from scanners, config drift, and IAM deltas and review posture at least monthly.
- ☐ **Prove it:** Provide the SSP, last assessment report, POA&M with owners/dates, and the monitoring calendar.

Common gaps: Shelf-ware SSPs, findings without accountable owners, and ignored drift alerts.

CM — Configuration Management

- ☐ **Do now:** Establish hardened baselines, require least functionality, and enforce formal change control.
- ☐ **Operate:** Run file-integrity monitoring, treat gold images as code, and hold emergency-change after-action reviews.
- ☐ **Prove it:** Produce baseline documents, change tickets with approvals, and FIM alerts with dispositions.

Common gaps: Local admin sprawl, leftover default services, and undocumented firewall/SD-WAN changes.

CP — Contingency Planning

- ☐ **Do now:** Set RTO/RPO for CJI systems and encrypt and test backups rather than assuming they work.
- ☐ **Operate:** Conduct quarterly restore tests including cloud failover and document lessons learned.
- ☐ **Prove it:** Provide backup configs, restore logs, and DR tabletop reports with action items.

Common gaps: No immutable/air-gapped copy, untested restores, and unverified vendor DR commitments.

IR — Incident Response

- ☐ **Do now:** Publish a CJIS-aligned IR plan with CSA/FBI notification triggers and assign roles.
- ☐ **Operate:** Drive detections from AU/CA into SOAR playbooks and preserve evidence with chain-of-custody.
- ☐ **Prove it:** Share the IR plan, recent drill notes, and tickets showing detect→contain→recover.

Common gaps: Unclear external-reporting thresholds and accidental evidence destruction during cleanup.

MA — Maintenance

- ☐ **Do now:** Pre-approve remote maintenance, vet technicians, and require session recording.
- ☐ **Operate:** Use time-bound vendor credentials, auto-terminate idle sessions, and verify systems post-maintenance.
- ☐ **Prove it:** Provide vendor rosters, maintenance logs/recordings, and verification checklists.

Common gaps: Persistent vendor accounts and unsupervised after-hours remote access.

MP — Media Protection

- ☐ **Do now:** Classify and label media, mandate encryption, and formalize sanitization/disposal procedures.
- ☐ **Operate:** Track chain-of-custody, block unapproved USB, and govern cloud snapshots/exports as media.
- ☐ **Prove it:** Produce media inventories, sanitization certificates, and DLP or device-control policies.

Common gaps: Forgotten cloud exports, unlabeled drives, and unmanaged removable media.

PE — Physical & Environmental Protection

- ☐ **Do now:** Restrict access to CJIS areas, escort visitors, and maintain entry logs.
- ☐ **Operate:** Use badges, CCTV, and tamper alarms and quarterly reconcile badge access with HR rosters.
- ☐ **Prove it:** Provide access lists, door/camera logs, and visitor records for sample periods.

Common gaps: Shared server rooms, unsecured comms closets, and unlogged contractor visits.

PL — Planning

- ☐ **Do now:** Maintain a current SSP mapping systems, data flows, owners, and control implementations.
- ☐ **Operate:** Update the SSP whenever significant changes occur and link it to change/project governance.
- ☐ **Prove it:** Show the SSP with revision history and cross-references to assets and controls.

Common gaps: Orphan systems and outdated data-flow diagrams.

PS — Personnel Security

- ☐ **Do now:** Set position risk levels, complete fingerprint-based screening before access, and collect signed access/NDAs.
- ☐ **Operate:** De-provision immediately on exit/transfer and apply sanctions and external-personnel controls consistently.
- ☐ **Prove it:** Provide screening records, agreement archives, and IAM offboarding time-to-disable metrics.

Common gaps: HR-to-IAM delays and contractors bypassing screening or agreements.

RA — Risk Assessment

- ☐ **Do now:** Perform a risk assessment emphasizing remote access, third-party services, and exposed data flows.
- ☐ **Operate:** Feed RA with vuln scans and exploited-in-the-wild intel and rapidly update treatment plans.
- ☐ **Prove it:** Share the RA report, scanner evidence, and a risk register with decisions and owners.

Common gaps: Static RA documents and exceptions without compensating controls.

SA — System & Services Acquisition

- ☐ **Do now:** Embed security requirements in SDLC and procurements and define external-service obligations up front.
- ☐ **Operate:** Enforce SAST/DAST/SBOM gates and manage unsupported components and supplier deliverables.
- ☐ **Prove it:** Provide contract clauses, SDLC gate logs, and supplier assurance artifacts.

Common gaps: Cloud lift-and-shift without CJIS clauses and no plan for EOL components.

SC — Systems & Communications Protection

- ☐ **Do now:** Segment CJIS networks, enforce deny-by-default at boundaries, and prohibit split tunneling.
- ☐ **Operate:** Manage external telecom interfaces, use authenticated proxies where appropriate, and maintain modern TLS/FIPS crypto.
- ☐ **Prove it:** Produce network diagrams, firewall/SD-WAN configs, and remote-access posture evidence.

Common gaps: Flat networks, legacy TLS, and uncontrolled egress paths.

SI — System & Information Integrity

- ☐ **Do now:** Set patch SLAs, deploy EDR/anti-malware everywhere, and require input validation on apps/feeds handling CJI.
- ☐ **Operate:** Automate patching with staged rollouts, run integrity monitoring, and triage alerts into IR.
- ☐ **Prove it:** Provide patch compliance reports, EDR coverage maps, and application validation evidence.

Common gaps: Ignored firmware updates, incomplete EDR rollouts, and missing validation on import jobs.

SR — Supply-Chain Risk Management

- ☐ **Do now:** Establish an SCRM policy and plan, form a cross-functional SCRM team, and add assessment/notification/audit clauses to contracts.
- ☐ **Operate:** Enforce key-custody boundaries, log exportability, personnel screening, and component authenticity/disposal with continuous verification.
- ☐ **Prove it:** Share contracts/SOWs, supplier assessment results, and evidence of log export and audit access.

Common gaps: Assuming FedRAMP/StateRAMP equals CJIS and unclear ownership of encryption keys.

Mobile Devices

- ☐ **Do now:** Publish mobile rules, require local device auth plus AA for direct CJI access, and enroll all devices in MDM/EMM.
- ☐ **Operate:** Enforce full-device encryption, remote wipe, and app control and avoid BYOD unless all controls are enforceable.
- ☐ **Prove it:** Provide MDM posture reports, lost-device response records, and AA configuration evidence.

Common gaps: "Temporary" unmanaged tablets, specialty devices outside MDM, and exceptions that become permanent.