Apptega

GUIDE

# CJIS Security Policy v6.0 Compliance Guide

Understanding and Implementing Security Requirements for Criminal Justice Information (CJI)

*Current as of August 19, 2025*

Apptega

Apptega

## 1. Introduction

CJIS Security Policy v6.0 establishes unified minimum security requirements for protecting Criminal Justice Information (CJI) at rest and in transit across Criminal Justice Agencies (CJAs), Noncriminal Justice Agencies (NCJAs), and their contractors. This guide is a practical, implementation-focused playbook to become compliant. It sets owners, parameters, measurable acceptance criteria, evidence locations, and audit mappings using CJIS terminology and policy areas.

## 1A. Beginner Quick-Start (First 30—90 Days)

### Days 1—15 (Program stand-up & SSP skeleton)

- Appoint: CSA/CSO liaison, Information Security Officer (ISO), Local Agency Security Officer(s) (LASO), Terminal Agency Coordinator(s) (TAC), System Owner(s).
- Define the CJI authorization boundary; draft the CJI data-flow map.
- Inventory Information Exchange Agreements (IEAs/IAAs) and vendor Security Addenda where unencrypted CJI access exists.
- Create the CJIS SSP skeleton: overview, boundary narrative, roles, inheritance/ outsourcing model, and brief policy-area narratives

### Days 16—45 (Tailoring & full draft)

- Run policy-area workshops to confirm applicability, parameters, acceptance criteria, and compensating measures.
- Establish advanced authentication, logging and alerting, change control, encryption and key management baselines.
- Complete the first full CJIS SSP draft by Day 45.

### Days 46—90 (Evidence & audit readiness)

- Populate the Evidence Register; conduct one IR tabletop and one restore drill.
- Perform an internal assessment aligned to agency audit checkpoints; update SSP and POA&M.
- Freeze an audit-ready CJIS SSP at least 14 days before external reviews.

## 2. Scope & Alignment

**Scope:** All people, processes, technology, and third parties that create, collect, process, store, transmit, or dispose of CJI within the boundary, including connected services.

**Assessment approach:** Use examine/interview/test methods mapped to CJIS controls and the agency's audit checklist.

**Inheritance/outsourcing:** Record provider obligations, verification of service-level settings, and residual responsibilities.

### 2A. Program Foundations & Definitions

- **Criminal Justice Information (CJI):** Data necessary for law enforcement and administration of criminal justice (e.g., biometric, identity history, case/incident, system transaction data).
- **Management Control:** Authority over day-to-day operations, policy, and personnel for systems handling CJI; must be clearly assigned and provable.
- **Security Addendum:** Mandatory contract terms for any private contractor with unencrypted CJI access.
- **Information Exchange Agreement (IEA/IAA):** Governs CJI sharing between agencies/entities, defining purpose, roles, controls, and incident coordination.
- **Advanced Authentication (AA): A**uthentication beyond username/password when required by policy (e.g., remote or non-local access).
- **Physically Secure Location vs. Controlled Area:** Distinct facility protection standards; compensating technical controls apply in Controlled Areas.

## 2B. Governance & Roles

- **CSA/CSO:** State or agency authority providing oversight, policy direction, and audits/inspections.
- **ISO:** Owns the security program, SSP, risk management, incident coordination, and audit response.
- **LASO:** Maintains endpoint inventory, local device posture, and control adherence.
- **TAC:** Oversees terminal programs, ensuring user/device eligibility and configuration.

**Acceptance criteria:** Formal appointments, documented duties, alternates named, and validated contact paths (at least quarterly).

## 2C. Facility Types & CJI Handling

- **Physically Secure Location:** Dedicated facility/area with access controls, escort rules, logs, and monitoring; preferred for CJI processing/storage.
- **Controlled Area:** Operational space with tailored physical protections and compensating technical controls (encryption, AA, device management).
- **Handling rules:** Encryption for CJI in transit and outside secure areas; clean desk; printer/fax controls; media custody; visitor escorting.

**Acceptance criteria:** Facility classification documented; signage and escort procedures enforced; printer/fax secure release; controls verified during walkthroughs.

Apptega

## 3. Policy Areas & Practices (CJIS v6.0)

### PA1 — Information Exchange Agreements

**Intent:** Formalize authority, purpose, controls, and responsibilities for CJI exchange.

**Minimums:** Current, signed IEAs/IAAs; explicit management control; incident coordination contacts.

**Implement — Procedural:** Agreement catalog; renewal calendar; change control; joint notification paths.

**Implement — Contractual:** Security Addendum for contractors with unencrypted CJI access; audit cooperation; data return/destruction.

- **Evidence:** Executed IEAs/IAAs; addenda; renewal logs.
- **Acceptance Criteria:** 100% exchanges governed; contacts validated quarterly.
- **Common Failures:** Stale MOUs; missing addenda.
- **Internal Audit Plan:** Sample 5–10 exchanges for scope, signatures, and terms.

### PA2 — Security Awareness Training

**Intent:** Ensure all personnel with CJI access understand obligations.

**Minimums:** Training before unescorted access; periodic refresh; role-based content (users, admins, contractors, LASO/TAC).

**Implement:** Onboarding gate; refresh cadence; phishing/reporting labs; developer secure coding for systems with CJI.

- **Evidence:** Completion rosters; scores; acknowledgments.
- **Acceptance Criteria:** 100% trained prior to unescorted access; refresh on schedule; remediation within 10 business days after failures.
- **Common Failures:** Access before training; out-of-cycle contractors.
- **Internal Audit Plan:** Trace 10 new users and 10 role changes.

## PA3 — Incident Response

**Intent:** Detect, analyze, contain, eradicate, recover, and report incidents affecting CJI.

**Minimums:** IR plan; defined roles; timely notifications to CJA/CSA; evidence preservation.

**Implement:** Playbooks (phishing, ransomware, exfiltration, insider, vendor breach); forensic readiness; after-action reviews with corrective actions.

- **Evidence:** IR plan; tickets; artifacts; notifications; AARs.
- **Acceptance Criteria:** Tabletop within last 12 months; 24×7 contact path; corrective actions tracked to closure.
- **Common Failures:** Delayed notification; weak evidence handling.
- **Internal Audit Plan:** Review 3 incidents end-to-end.

## PA4 — Auditing & Accountability

**Intent:** Enable detection and investigation via audit trails.

**Minimums:** Required events captured; synchronized time; retention (≥1 year with ≥90 days immediately available).

**Implement:** Central SIEM; immutable storage; review cadence; alerting runbooks; ingestion health checks.

- **Evidence:** Log configs; retention settings; admin event samples; alert tickets.
- **Acceptance Criteria:** Required events on 100% in-scope systems; daily ingestion health checks; online availability for recent logs.
- **Common Failures:** Missing admin events; insufficient retention.
- **Internal Audit Plan:** Validate 5 key systems; review alert triage and closure SLAs.

## PA5 — Access Control

**Intent:** Enforce least privilege and authorized access to CJI.

**Minimums:** Account lifecycle; separation of duties; session control; portable media restrictions.

**Implement — Procedural:** Role catalog; joiner–mover–leaver within 24 hours; quarterly access reviews; privileged approvals; break-glass governance.

**Implement — Technical:** SSO and AA where required for remote/non-local access; PAM/JIT elevation with session recording; segmentation; device trust for remote endpoints.

- **Evidence:** RBAC matrix; recertification results; AA/MFA coverage; PAM recordings.
- **Acceptance Criteria:** 100% AA/MFA on remote/admin; idle timeout ≤15 minutes; absolute session ≤12 hours; orphaned accounts = 0.
- **Common Failures:** Shared admin credentials; unmanaged tokens.
- **Internal Audit Plan:** Sample 25 users and 10 admins.

## PA6 — Identification & Authentication (Advanced Authentication)

**Intent:** Uniquely identify and strongly authenticate users/devices/services.

**Minimums:** Unique IDs; credential standards; AA where required; FIPS-validated cryptography for credential storage/transit.

**Implement:** Central identity; phishing-resistant MFA where feasible; device certificates; secret rotation SLAs; PAM for elevation.

- **Evidence:** AA/MFA coverage reports; device trust inventories; secret rotation logs.
- **Acceptance Criteria:** 100% AA for required access paths; zero shared credentials; secrets rotated within SLA.
- **Common Failures:** Exceptions without compensations; unmanaged service accounts.
- **Internal Audit Plan:** Review 20 identities and 10 service accounts.

## PA7 — Configuration Management

**Intent:** Maintain hardened baselines and controlled change.

**Minimums:** Baselines; approvals; code/config review; drift detection; inventory accuracy.

**Implement:** Infrastructure-as-code with PR reviews; hardened images; config scanning; drift alerts; emergency change path; CMDB governance.

- **Evidence:** Baselines; change records; drift reports; PR trails; inventory.
- **Acceptance Criteria:** Baseline via IaC to 100% scope; drift alerts ≤24 hours; CMDB accuracy ≥98%.
- **Common Failures:** Manual drift; no rollback/testing.
- **Internal Audit Plan:** Sample 10 changes; compare deployed vs. baseline.

## PA8 — Media Protection

**Intent:** Safeguard CJI on physical/digital media.

**Minimums:** Labeling; tracking; encryption; controlled transport; sanitization/disposal.

**Implement:** Chain of custody; FIPS-validated encryption on portable media; vendor destruction with certificates.

- **Evidence:** Media logs; encryption configurations; destruction certificates.
- **Acceptance Criteria:** 100% encrypted portable media; disposal within SLA with certificates.
- **Common Failures:** Untracked exports; lost media.
- **Internal Audit Plan:** Trace 10 items from issuance to disposal.

## PA9 — Physical Protection

**Intent:** Limit physical access and protect facilities hosting CJI.

**Minimums:** Controlled areas; badges/escorts; visitor logs; environmental safeguards.

**Implement:** Access reviews; surveillance/alarm coverage; tamper-evident seals; shipping/receiving controls.

- **Evidence:** Badge lists; visitor logs; camera retention settings; environmental test results.
- **Acceptance Criteria:** Visitor logs retained; escorts enforced; environmental tests current.
- **Common Failures:** Shared badges; uncontrolled deliveries.
- **Internal Audit Plan:** Walkthrough; sample logs and camera coverage.

## PA10 — System & Communications Protection & Information Integrity

**Intent:** Protect CJI in transit and at rest; enforce boundaries; assure integrity.

**Minimums:** FIPS-validated encryption when CJI is outside secure areas or in transit; boundary protections; integrity checks.

**Implement:** TLS/SSH standards; web and network protections (WAF/IDS/IPS); micro-segmentation; DNS/email protections; key management SOP (KMS/HSM); deny-by-default egress.

- **Evidence:** Cipher configurations; key rotation logs; segmentation diagrams; rulesets.
- **Acceptance Criteria:** Strong ciphers; managed interfaces; changes via approved records; key rotation within policy.
- **Common Failures:** Non-FIPS crypto; flat networks; open egress.
- **Internal Audit Plan:** Validate crypto; inspect segmentation; review egress exceptions.

## PA11 — Formal Audits

**Intent:** Demonstrate sustained compliance under CSA/agency audits.

**Minimums:** Audit preparation; evidence collection; corrective action tracking.

**Implement:** Annual internal audit; readiness package; CAP/POA&M governance with due dates and owners.

- **Evidence:** Internal audit reports; corrective action logs; inspection correspondence.
- **Acceptance Criteria:** Prior findings closed or on-track with documented milestones.
- **Common Failures:** Disorganized evidence; stale corrective actions.
- **Internal Audit Plan:** Re-test prior findings and spot-check new controls.

## PA12 — Personnel Security

**Intent:** Trustworthy personnel and clean separations.

**Minimums:** Fingerprint-based checks before unescorted access to unencrypted CJI; NDAs; periodic reinvestigation per CSA direction.

**Implement:** Pre-access screening; role-based rescreen cadence; offboarding within 24 hours; insider risk awareness.

- **Evidence:** Screening records; offboarding tickets; access removal proofs.
- **Acceptance Criteria:** Screening complete before unescorted access; deprovision ≤24 hours; lingering access = 0.
- **Common Failures:** Access prior to screening; delayed offboarding.
- **Internal Audit Plan:** Sample 10 hires and 10 exits.

## PA13 — Mobile Devices & Tablets

**Intent:** Control mobile endpoints that access/store CJI.

**Minimums:** Device management; encryption; screen lock; remote wipe; storage rules.

**Implement:** MDM with compliance policies; containerization; jailbreak/root detection; camera/Bluetooth restrictions in secure areas where required.

- **Evidence:** MDM compliance reports; encryption settings; wipe logs.
- **Acceptance Criteria:** 100% managed and encrypted; lost/stolen devices wiped within SLA.
- **Common Failures:** BYOD without controls; unmanaged apps.
- **Internal Audit Plan:** Sample 20 devices for posture.

## PA14 — Wireless

**Intent:** Secure wireless used in or near CJI environments.

**Minimums:** Strong authentication and encryption; segmentation; rogue detection.

**Implement:** 802.1X/EAP-TLS; WPA3-Enterprise where supported; dedicated CJI SSID/VLANs; WIPS monitoring.

- **Evidence:** Controller configs; certificate inventories; WIPS alerts.
- **Acceptance Criteria:** Only approved SSIDs; CJI WLAN segmented; rogue events triaged within SLA.
- **Common Failures:** PSK reuse; guest bridging into CJI networks.
- **Internal Audit Plan:** Review configs and WIPS telemetry.

## PA15 — Remote Access

**Intent:** Control non-local access to CJI.

**Minimums:** Advanced Authentication; encryption; session protection; device posture enforcement.

**Implement:** VPN or ZTNA with device trust; split-tunnel policy; idle/absolute timeouts; restricted clipboard/drive mapping where required.

- **Evidence:** VPN/ZTNA configs; AA coverage; session records.
- **Acceptance Criteria:** 100% AA; timeouts enforced; admin remote sessions wrecorded.
- **Common Failures:** Exceptions without compensations; unmanaged home devices.
- **Internal Audit Plan:** Sample 10 remote sessions and confirm posture.

## PA16 — Virtualization & Containers

**Intent:** Secure hypervisors, VMs, and containers processing CJI.

**Minimums:** Isolation; hardened templates; admin separation; logging.

**Implement:** Host/guest hardening; signed images; east–west segmentation; registry controls; least-privilege runtime.

- **Evidence:** Baselines; change logs; segmentation ACLs; hypervisor/container logs.
- **Acceptance Criteria:** Only signed images; privileged operations logged; isolation by zone.
- **Common Failures:** Flat east–west; shared admin accounts.
- **Internal Audit Plan:** Compare VM/container baselines to running configs.

## PA17 — Cloud Computing

**Intent:** Ensure cloud use meets CJIS requirements and CSA expectations.

**Minimums:** Executed Security Addendum (through the CSA) when required; CJI location controls; screened administrators; audit cooperation; encryption & key management aligned to CJIS.

**Implement:** Data residency constraints; provider control mapping; verification of service-level settings (admin MFA/AA, logging export, storage encryption, public object defaults).

- **Evidence:** Executed addendum; architecture diagrams; logging exports; KMS settings; admin AA evidence.
- **Acceptance Criteria:** CJI stored/processed only in permitted locations; provider admin access logged; keys managed per SOP.
- **Common Failures:** Assuming provider compliance without validating configuration.
- **Internal Audit Plan:** Review provider attestations and your configuration against policy.

## PA18 — Outsourcing (Security Addendum)

**Intent:** Govern third parties with access to CJI.

**Minimums:** Security Addendum for any unencrypted CJI access; clear roles; screening requirements; incident notice SLAs.

**Implement:** TPRM tiers; audit rights; software vendor patch/SBOM expectations; offboarding/return/destruction terms.

- **Evidence:** Contracts; addenda; screening attestations; audit results.
- **Acceptance Criteria:** 100% required addenda in place; timely incident/vulnerability notices; complete offboarding.
- **Common Failures:** Missing addenda; unclear management control.
- **Internal Audit Plan:** Sample 5 critical vendors end-to-end.

## 4. Authorization Boundary & CJI Data-Flow Mapping

Document components, interfaces, trust zones, external services, and where CJI flows, rests, and leaves. Maintain records of processing (sources, stores, transmissions, recipients). Update upon material change. Include the diagram and narrative in the SSP by Day 15; keep synchronized through the Day-45 full draft and pre-audit freeze.

## 5. CJIS SSP — Canonical Narratives

Write the SSP as cohesive prose covering: system overview and mission; boundary and inventory; CJI categories and lifecycle; roles and governance; inheritance and outsourcing with verification of provider settings; policy-area implementations; identity/AA, zoning/egress, cryptography, logging, backups, vulnerability management; assessment status and findings; change and baselines; vendors and sub-tiers.

**SSP timing:** Skeleton Days 1–15 → full draft by Day 45 → audit-ready freeze at least 14 days pre-audit; update on boundary/technology/CJI changes or after POA&M closures that change narratives.

## 6. Applicability, Acceptance Criteria & Audit Mapping

Maintain a definitive record for each control topic with applicability, implementation summary, parameter values, measurable acceptance criteria, audit checkpoints, inheritance type, and evidence location.

*Example excerpt (illustrative):*

| Policy Area | Control/Topic | Applicable | Implementation Summary | Parameters | Acceptance Criteria | Inheritance | Evidence |
|---|---|---|---|---|---|---|---|
| PA5 | Least Privilege & Recerts | Y | RBAC via SSO; quarterly recerts | Idle 15m; lockout 5/30m | Users mapped; recerts ≤90d; deprovision ≤24h | System | GRC/AC/Recert_Q2.csv |
| PA4 | Audit Events & Retention | Y | SIEM; immutable storage | Retention ≥12m; 90d online | Required events 100%; ingestion health daily | Hybrid | SecOps/SIEM/health.png |
| PA6 | Advanced Authentication | Y | AA on remote/admin; device trust | — | 100% coverage; exceptions time-bound | Enterprise | IAM/AA_Coverage.csv |
| PA10 | FIPS-Validated Crypto | Y | TLS/SSH; KMS/HSM | Rotation 12m | Strong ciphers; keys per SOP | Hybrid | Crypto/KMS_Std.pdf |
| PA12 | Screening/Offboarding | Y | Fingerprint checks; JML | Deprovision 24h | No access pre-screen; exits clean | System | HR/Sec/Offboard.xlsx |

## 7. Control Parameter Defaults (Organization-Specific Settings)

- **Sessions & Access:** Idle 15 minutes; absolute 12 hours; failed attempts 5 within 30 minutes; lockout 30 minutes; admin JIT 60 minutes.
- **Cryptography:** FIPS-validated modules; TLS 1.2+ strong suites; at-rest AES-256; key rotation every 12 months; keys in KMS/HSM.
- **Logging:** Required event set; retention ≥12 months (≥90 days immediately available); clock drift ≤5 minutes; daily ingestion health alerts.
- **Patching:** Critical ≤15 business days; High ≤30; Medium ≤60; Low ≤90; exceptions ≤90 days with compensations.
- **Backups:** Daily incrementals; weekly full; immutability 30 days; quarterly restore test meeting RTO/RPO.
- **Identity:** Deprovision ≤24 hours; service accounts owned and rotated ≤90 days; device trust for admin endpoints.
- **Data Handling:** Labeling; approved export channels; deletion within 30 days after trigger.
- **Vendors:** Incident notice ≤72 hours; SBOM on request; annual reassessment; right to audit.

## 8. Evidence Register

| Artifact | Policy Areas | Location/Path | Owner | Format | Retention |
|---|---|---|---|---|---|
| Access Recert Q2 | PA5 | GRC/ Recerts/2025Q2 | IAM Lead | CSV + sign-off PDF | 6 years |
| AA Coverage Report | PA5/PA6/PA15 | IAM/Reports/AA.csv | IAM Lead | CSV/PNG | 3 years |
| SIEM Rule Pack v5 | PA3/PA4/PA10 | SecOps/SIEM/rules | SecOps | JSON | Current + 1 year |
| Restore Drill 2025-05 | PA10 ops | Resilience/ Tests/2025-05 | DR Lead | PDF | 6 years |
| Firewall Ruleset | PA10 | Net/Firewall/Ruleset. yaml | NetSec | YAML | Current + 1 year |
| IEA/IAA Catalog | PA1/PA18 | Legal/Sec/IEAs.xlsx | Legal | XLSX | Active + 6 years |
| Security Addenda | PA17/PA18 | Legal/Sec/Addenda/ | Legal | PDF | Active + 6 years |

## 9. Continuous Monitoring Plan

- **Daily:** SIEM ingestion health; critical alerts triage; AA/MFA coverage exceptions; EDR coverage check.
- **Weekly:** Vulnerability scans; failed backups; admin activity review sample; WIPS rogue events review.
- **Monthly:** Access review roll-up; config drift review; patch SLA dashboard; egress rule review; IEA/IAA change check.
- **Automations:** Open tickets on ingestion failures, missing EDR/AA, encryption drift, expired exceptions, or addendum/IEA gaps.
- **Reporting:** Dashboard to ISO with owners and due dates.

## 10. POA&M Workflow & Risk Acceptance Criteria

- Identify → Record (severity, owner, due date, milestones) → Treat (remediate/compensate/time-bound accept) → Verify with evidence → Report.
- Targets: Critical ≤15 business days; High ≤30; Medium ≤60; Low ≤90.
- Risk acceptance requires compensating controls, explicit expiry, and leadership approval; reminders 14 days before expiry. Update SSP narratives when closures materially change implementations.

## 11. Cloud & Hosting (Shared Responsibility, IAA & Security Addendum)

Classify each control as inherited, shared, or system-specific. Capture provider attestations, data locations, key management model, logging/egress controls, incident notice SLAs, and subprocessor transparency. Verify service-level settings (admin AA, log exports, storage encryption, public object defaults). Integrate SSO/AA and SIEM exports. Reflect provider obligations in IEAs/IAAs and Security Addenda.

## 12. Training & Awareness Program (Role-Based)

Onboarding ≤30 days; periodic refresh; quarterly micro-modules. Tracks: workforce baseline; Admin/IT; Developers (secure coding/SDLC); Security Ops; Executives; Vendors. Measure completion ≥98%, phishing failure trend down, remediation ≤10 days, retraining after incidents or role changes. Summarize scope and metrics in the SSP.

## 13. Vendor & Supply Chain Coverage (CJIS Outsourcing)

Tier suppliers handling CJI; define artifacts. Contract for security clauses; breach and vulnerability notice SLAs; SBOM delivery; audit rights; sub-tier transparency. Monitor renewals, external attack surface, incident sharing, and change notifications. Offboard with data return/destruction and credential/certificate revocation; preserve logs. Name critical suppliers and obligations in the SSP.

## 14. SDLC Gatekeeping & Pipeline Controls

Embed controls across delivery:

- **Plan:** Threat modeling; security non-functional requirements; acceptance criteria.
- **Build:** SAST/SCA; secrets scanning; artifact signing.
- **Test:** DAST; container and IaC scans.
- **Release:** Change approval; drift checks; rollout/backout plans.
- **Operate:** Observability; WAF/IDS; IaC drift monitors.
- **Blocking gates:** failing SAST/SCA/secrets/IaC checks block merge or release unless a time-bound exception with compensations is approved. Keep pipeline logs and signatures as evidence.

## 15. Evidence Sampling Plans (Internal Audit)

- **Access (PA5):** Sample 25 users and 10 admins; check RBAC mapping, AA status, last login, and deprovision proofs.
- **Changes (PA7):** Sample 10 change records; confirm approvals, PR reviews, rollback, and deployed state vs. baseline.
- **Logging (PA4):** Sample 5 CJI systems; required events, retention, and alert handling.
- **Backups/Restores (PA10):** Perform 3 restores from different tiers; confirm RTO/RPO met.
- **Vulnerabilities (PA10/SI-like practices):** Sample 20 hosts; verify patch SLA adherence and exception expiry.
- **Vendors (PA17/PA18):** Review 5 critical vendors; confirm addenda, AA evidence, logging, data location, incident notices.

## 16. Common Pitfalls

Assuming provider inheritance without validating settings; missing parameter values that make requirements untestable; logging without alert use-cases; weak joiner–mover–leaver; unmanaged service accounts; untested restore; vague third-party terms; scattered evidence and undefined retention. Address mitigations to these pitfalls in SSP narratives.

## 17. Quick Reference Summary

| Area | Core Artifacts | Examples |
|---|---|---|
| PA1 | IEA/IAA catalog; addenda | Management control; incident contacts |
| PA2 | Training matrix; completion records | Role-based training; secure coding |
| PA3 | IR plan; playbooks; AARs | Evidence preservation; notifications |
| PA4 | Log standard; SIEM rules; retention configs | Immutable logs; admin event capture |
| PA5 | RBAC matrix; access reviews; PAM/JIT logs | AA on remote/admin; session management |
| PA6 | AA policy; device certificates | SSO; PAM; service accounts |
| PA7 | Baselines; change records; drift reports | IaC; hardened images |
| PA8 | Media logs; encryption; destruction certs | Chain of custody; TLS transfers |
| PA9 | Badge/CCTV logs; visitor logs | Visitor management; locks |
| PA10 | Crypto/KMS records; segmentation | WAF; IDS/IPS; TLS configs |
| PA11 | Internal audit reports; CAP | Readiness packs; evidence lists |
| PA12 | Screening; offboarding tickets | JML; badge disable; device wipe |
| PA13 | MDM compliance; wipe logs | Containerization; posture rules |
| PA14 | WLAN configs; WIPS alerts | 802.1X/EAP-TLS; WPA3-Ent |
| PA15 | VPN/ZTNA configs; session logs | Device trust; split-tunnel policy |
| PA16 | Baseline images; hypervisor logs | Signed images; isolation |
| PA17 | Cloud diagrams; logging exports; KMS | Admin AA; storage encryption |
| PA18 | Contracts; security addenda; audit reports | SBOM; patch SLAs |

## 18. Self-Assessment & Leadership Attestation

*Use a clear, four-status scale for planning and reporting:*
**Compliant (C) / Partially Compliant (PC) / Not Compliant (NC) / Not Applicable (N/A).**

### When "N/A" is allowed (and how to prove it)

Use **N/A** only when a control topic is truly out of scope for the assessed boundary. Record a short, evidence-backed rationale using one (or more) of these categories:

- **OOS (Out of Scope by Boundary)**: The function/technology does not exist in the CJIS boundary (e.g., no wireless in secure areas).
- **INH (Fully Inherited):** The requirement is met entirely by a provider under a valid agreement, with management control and verification of service-level settings documented.
- **FAC (Facility Type):** The control applies only to a facility type you do not operate (e.g., no Controlled Area—only a Physically Secure Location).
- **ROLE (Role/Program Absence):** The requirement pertains to a user/device role your boundary does not authorize (e.g., no mobile device access to CJI).
- **UR (Jurisdictional Directive):** CSA/agency directive explicitly excludes the scenario from your boundary.

**Not permitted:** Marking **N/A** because implementation is difficult, because a compensating control exists (that is **PC** or **C** once implemented), or because you intend to decommission a system later. If the control is applicable but unmet, use **NC** (or **PC** if partially implemented and you can demonstrate effectiveness).

### Governance for N/A

- N/A decisions must reference the SSP section and boundary diagram that substantiate out-of-scope status.
- Require ISO approval; where appropriate, capture CSA/CSO acknowledgement (e.g., via email or audit note).
- Revalidate at least annually and on any material change (boundary, facility, connectivity, vendors).

### Leadership attestation (what to include)

A brief narrative signed by the ISO (and executive, if required) covering: boundary identifier and version, assessment dates and method, overall status summary, list of N/A items with rationale codes, top risks, and a pointer to the current POA&M.

### Tracker format (illustrative):

| Policy Area / Control Topic | Status (C/PC/ NC/N/A) | Rationale (for N/A use OOS/INH/FAC/ ROLE/JUR) | Evidence Link | Owner | POA&M ID (if PC/ NC) |
|---|---|---|---|---|---|
| PA5 – Least Privilege & Recerts | C | — | GRC/AC/Recert_Q2.csv | IAM Lead | — |
| PA6 – Advanced Authentication (Remote Admin) | PC | — | IAM/AA_Coverage.csv | IAM Lead | POA&M-2025-017 |
| PA4 – Admin Event Logging | NC | — | SecOps/SIEM/health.png | SecOps Mgr | POA&M-2025-022 |
| PA14 – Wireless in Secure Areas | N/A | OOS (no WLAN in PSL; see SSP §2C, Diagram D-3) | Facilities/Designs/PSL_ D3.pdf | Facilities Sec | — |
| PA17 – Cloud Admin MFA (Provider Console) | N/A | INH (provider-admin path governed by executed Addendum; verified settings in §11) | Legal/Addenda/Cloud.pdf | Vendor Mgmt | — |
| PA13 – Mobile Device Access to CJI | N/A | ROLE (policy prohibits mobile CJI access) | Policy/Mobile_NoCJI.pdf | LASO | — |

### Attestation checklist

- [ ] Status inventory complete for all policy areas/topics
- [ ] Every **N/A** has a rationale code, an SSP/diagram reference, and a durable evidence link
- [ ] **PC/NC** items map to the **POA&M** with owners, milestones, and due dates
- [ ] Contacts for ISO/LASO/TAC verified and current

### SSP tie-in

List **N/A** items and their rationale codes in the SSP's relevant sections (policy-area narratives and boundary description). Update whenever the boundary, facilities, connectivity, or vendor landscape changes.

## 19. CJIS Audit Readiness & Agency Inspections

Prepare a compact package: boundary diagram; SSP (current); Evidence Register index with links; last internal audit and CAP; IR tabletop/AAR summaries; IEA/IAA and addenda list; critical vendor list with obligations. Ensure points of contact (ISO, LASO, TAC) are available and contact details are current. Rehearse 30-minute "system walk-through" and 15-minute evidence navigation.

## 20. References & Resources

*FBI CJIS Security Policy v6.0 (official publication)*
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

*CJIS Security Addendum (contract language)*
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/security-addendum

*CJIS Policy Resource Center (implementation aids, FAQs)*
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

*NIST National Checklist Program (baseline configuration checklists)*
https://nvd.nist.gov/ncp/repository

*National Vulnerability Database*
https://nvd.nist.gov/

Apptega

# Apptega Product Features

16+ Security Frameworks

One-Click Reporting

Automated Alerts & Notifications

API & Application Connectors

Automated Framework Crosswalking

Real-Time Compliance Scoring

Restricted Auditor View

Single Sign-On Connectivity

Policy & Plan Templates

Automated Risk Assessments

Document Repository for Artifacts

Multi-Tenant Environment

Apptega

# About Apptega

A perennial G2 leader across various cybersecurity categories, Apptega is the cybersecurity and compliance platform purpose-built for security providers who are growing lucrative security practices, creating stickier customer relationships, and winning more business from competitors.

With Apptega's end-to-end platform, IT providers can:

1. Build continuous compliance offerings that set them apart, retain customers, and grow their ARR.
2. Build and manage world-class cybersecurity and compliance programs for their clients.
3. Increase the capacity and efficiency of their existing team so they can service 2–3× more customers.
4. Assess, measure, and manage their own security programs against a standard set of industry-leading frameworks.

To learn more, visit apptega.com

Visit apptega.com