Barkrum

RESOURCE · QUICK CHECKLIST

CJIS Readiness Quick Checklist

A fast self check against the modernized CJIS Security Policy, before the audit reaches you.

This checklist reflects the CJIS Security Policy version 6.1, dated June 25, 2026, which continues the major modernization introduced in version 6.0. **It is a starting point, not a substitute for a full assessment.** Each item you cannot check is a gap worth a closer look before an audit finds it.

> **Where things stand:** *version 6.0 reorganized the policy around the NIST 800-53 control families and introduced priority tiers P1 through P4. Priority 1 controls, including multifactor authentication, have been sanctionable since October 1, 2024. Formal auditing under the modernized policy has been active since October 1, 2025, and full compliance across all remaining controls is required by September 30, 2027.*

IDENTITY AND ACCESS · The most emphasized and most audited area	
☐ **Multifactor authentication in place.** MFA protects all access to criminal justice information, including from legacy web applications and portals, not only email and VPN.	IA-2, IA-2(1); P1, sanctionable now
☐ **Every user uniquely identified.** Each person with access has a unique account; shared logins are eliminated.	IA-2, IA-4
☐ **Account lifecycle managed.** Access is granted, changed, and promptly removed as people join, change roles, or leave, ideally automatically.	AC-2
☐ **Least privilege enforced.** Users hold only the access their role requires, and administrator rights are limited and separated from daily use.	AC-5, AC-6
☐ **Authenticator controls current.** Password and authenticator policies follow the modernized guidance rather than outdated forced-rotation habits.	IA-5

AUDITING AND ACCOUNTABILITY · Prove control, do not just assert it	
☐ **Audit logging enabled.** Systems that access, store, or transmit criminal justice information generate audit logs.	AU-2, AU-3
☐ **Logs actually reviewed.** There is a defined process and cadence for reviewing logs, with evidence that review occurs.	AU-6
☐ **Logs retained and protected.** Audit records are kept long enough to investigate an incident and are protected from tampering.	AU-9, AU-11

TECHNICAL PROTECTIONS · Encryption, boundaries, and integrity	
☐ **Encryption applied to CJI.** Criminal justice information is encrypted at rest and in transit to the required standard.	SC-8, SC-13, SC-28
☐ **Network boundaries controlled.** Firewalls and network segmentation separate criminal justice information from general traffic.	SC-7
☐ **Systems patched and monitored.** Flaws are remediated promptly, malicious code protection is active, and systems are monitored.	SI-2, SI-3, SI-4

PHYSICAL PROTECTION · A compliance requirement, tested not just installed	
☐ **Secure locations controlled.** Rooms housing CJI systems have card reader access, cameras, and logged	PE-3, PE-6

	visitor escort procedures.	
☐	**Physical controls periodically tested.** Access controls are reviewed and tested on a schedule, not only installed once.	PE-3
☐	**Equipment protected.** Servers and network gear that handle CJI are physically secured against unauthorized contact.	PE-3

PERSONNEL AND TRAINING · The people side of compliance

☐	**Personnel screened.** Everyone with access to criminal justice information has passed fingerprint-based background screening.	PS-3
☐	**Security awareness training current.** Training is delivered within six months of assignment and repeated biennially, with records retained.	AT-2
☐	**Access removed at separation.** Termination and role-change procedures revoke access to criminal justice information promptly.	PS-4, PS-5

INCIDENT RESPONSE AND CONTINUITY · Ready before, not during

☐	**Incident response plan in place.** A documented plan covers detection, response, and reporting to the CJIS Systems Agency.	IR-1, IR-8
☐	**Contingency and backup tested.** Continuity plans and data backups exist and have been tested by an actual restore.	CP-2, CP-9, CP-10

GOVERNANCE AND SUPPLY CHAIN · The v6.0 shift to continuous accountability

☐	**Security roles assigned.** A Local Agency Security Officer and Terminal Agency Coordinator are formally designated.	PL-1, PS-2
☐	**Agreements executed.** CJIS management control and information exchange agreements are in place with partners and vendors.	SA-9
☐	**Vendor risk managed.** Contractors and vendors with access are vetted and bound by the CJIS Security Addendum, with supply chain risk managed.	SR-1, SR-6
☐	**System documentation maintained.** A system security plan or equivalent documents how criminal justice information is protected.	PL-2, CA-2

Not sure where you stand?

A Barkrum CJIS Readiness Assessment turns this checklist into a measured gap analysis against the current policy, mapped to the NIST 800-53 control families and prioritized by the sanctionable items first, with a clear roadmap to the 2027 deadline.

www.Barkrum.com

Educational resource based on the FBI CJIS Security Policy v6.1 (June 25, 2026). Audit baselines and transition timing can vary by state; confirm the exact baseline with your CJIS Systems Agency. In Florida, this is the FDLE. General guidance, not a guarantee of compliance or a substitute for a full assessment.