SmartSuite

Framework / Cybersecurity / Other

FBI CJIS Security Policy v6.1

The FBI CJIS Security Policy v6.1 sets minimum security requirements for agencies and contractors that access or handle Criminal Justice Information.



What it is

The FBI's Criminal Justice Information Services (CJIS) Security Policy, version 6.1 dated June 25, 2026, sets the minimum security requirements for every agency and contractor that accesses FBI CJIS systems or that processes, stores or transmits Criminal Justice Information (CJI). It applies to criminal justice agencies, noncriminal justice agencies and interface agencies, and since version 6.0 (December 27, 2024) it has been a public document.

At a glance

PUBLISHER
Federal Bureau of Investigation (FBI)

TYPE
Framework

VERSION
CJIS Security Policy v6.1 (June 25, 2026); v6.0 completed modernization (December 27, 2024)

EFFECTIVE
June 25, 2026 (v6.1); Priority 1 sanctionable since October 1, 2024

DOMAIN
Cybersecurity

FAMILY
Other

REGION
United States

INDUSTRY
Government & Public Sector

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: le.fbi.gov/cjis-division/cjis-security-policy-resource-center

Why it matters

- **One national minimum** The Policy is always the minimum standard; state, local, Tribal, territorial and federal agencies may adopt stricter rules (section 1.3).
- **Named roles and owners** Sections 3.2.1 to 3.2.13 define the CSA, CSO, Terminal Agency Coordinator, Agency Coordinator, CSA ISO and others, so each duty has an owner.
- **Priorities that guide audits** Each modernized control is marked Existing or Priority 1 to 4, and only existing and Priority 1 requirements are sanctionable until September 30, 2027 (section 1.4).
- **A route for contractors** Management control agreements and the CJIS Security Addendum let private contractors support criminal justice functions under FBI-approved controls (sections 3.2.6 and 5.1, Appendix H).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CJIS Security Policy

CJI Boundary and Exchange Agreements

Record where CJI is stored and transmitted, with each information exchange agreement, management control agreement and Security Addendum (5.1, Appendix H).

Requirement Library by Priority

Track requirements by policy area with the Existing or Priority 1 to 4 marking, owner, status and review date (1.4).

Personnel Screening and Training Records

Track screening completion, access approvals, annual training and the three-year training records (PS-3, AT-2, AT-4).

Access, MFA and Audit Log Evidence

Hold account reviews, multi-factor authentication proof and weekly audit record review sign-offs (AC-2, IA-2, AU-6).

Incident Reporting

Record suspected incidents with discovery time, the one-hour report and notices to the CSO and the FBI CJIS ISO (IR-6).

Audit Readiness Reporting

Report evidence coverage by policy area and by sanctionable priority ahead of audits.

Common framework mappings

FedRAMP Rev. 5 | FISMA | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-171 Rev. 3 | NIST 800-53 Rev.5 | SOC 2

Official resources

CJIS Security Policy v6.1 (PDF)

The FBI's current CJIS Security Policy, version 6.1 dated June 25, 2026, including the Security Addendum in Appendix H.

le.fbi.gov/file-repository/cjis_security_policy_v6-1_20260625-1.pdf

CJIS Security Policy Resource Center

The FBI's hub for the current policy, the Requirements Companion Document, use cases and links of importance.

le.fbi.gov/cjis-division/cjis-security-policy-resource-center

NIST IR 8523: Multi-Factor Authentication for Criminal Justice Information Systems

NIST's September 2025 guidance on implementing multi-factor authentication for CJI, listed on the FBI's resource center.

csrc.nist.gov/pubs/ir/8523/final

28 CFR Part 20: Criminal Justice Information Systems

The federal regulation behind the Policy's rules for CHRI dissemination and the Security Addendum (28 CFR 20.33).

ecfr.gov/current/title-28/chapter-I/part-20

Frequently asked questions

Who must follow the CJIS Security Policy?

The Policy applies to all entities with access to, or operating systems used to process, store or transmit, Criminal Justice Information (section 1.2). That includes criminal justice agencies, noncriminal justice agencies, interface agencies and private contractors under a management control agreement or the CJIS Security Addendum (sections 3.2.4 to 3.2.6).

What is Criminal Justice Information (CJI) and what is CHRI?

CJI is all FBI CJIS-provided data needed by law enforcement and civil agencies, in five categories: biometric, identity history, biographic, property and case or incident history data (section 4.1). Criminal history record information (CHRI) is a subset with extra controls, and 28 CFR Part 20 governs its dissemination (4.1.1). Ten NCIC restricted files are protected as CHRI (4.2.2).

Which requirements can be sanctioned today?

Since October 1, 2024, requirements that existed before the policy modernization and all Priority 1 requirements are sanctionable. Priority 2, 3 and 4 requirements are in zero-cycle status until September 30, 2027 (section 1.4). Version 6.1, dated June 25, 2026, incorporates the year-2025 changes approved by the APB in 2026 the 2026 Sanctionable.

Updated Oct 15, 2026 © 2026 SmartSuite Inc. All rights reserved.

What does the Policy require for authentication, encryption and incident reporting?

Multi-factor authentication is required for privileged and non-privileged accounts (IA-2(1) and (2)). CJI outside physically secure locations uses FIPS 140-3 certified cryptographic modules or FIPS 197 (AES) with symmetric keys of at least 256 bits, and FIPS 140-2 certificates are not accepted after September 21, 2026 (SC-13, SC-28). Suspected incidents are reported within one hour of discovery (IR-6).

How do contractors and cloud providers handle CJI?

Before exchanging CJI, agencies put formal agreements in place that specify security controls (section 5.1). Private contractors performing criminal justice functions sign the CJIS Security Addendum (Appendix H), authorized by 28 CFR 20.33(a)(7). CJI may be stored in cloud environments only within the physical boundaries of an APB-member country and under the legal authority of an APB-member agency (SC-28).

License included / downloadable: Yes The FBI publishes the CJIS Security Policy, version 6.0 and later, as a public document that may be posted and shared without restrictions (section 1.5), and it is included with the platform for reference.

Full framework page and mappings: smartsuite.com/frameworks/cjis-security-policy-criminal-justice-information-services-security