



Security Control Mapping of CJIS Security Policy Version 5.5 Requirements to NIST Special Publication 800-53 Revision 4 06/01/2016

At the request of the Advisory Policy Board (APB) Security & Access (SA) Subcommittee, the FBI CJIS Information Security Officer (ISO) Program Office began a project to map the requirements of the CJIS Security Policy to the security controls found in the NIST Special Publication 800-53 Revision 4. This document is the culmination of that project and is intended to provide a cross-reference between security requirements focused on the protection of criminal justice information (CJI) and federal information security requirements.

While the CJIS Security Policy has its genesis in federal guidelines, those requirements have been shaped by the shared management philosophy of the APB process in which each local, state, tribal, and federal law enforcement agency are stakeholders. Additionally, noncriminal justice agencies (NCJAs) follow the same standard when accessing civil information for authorized purposes.

This document should only be used as a reference when deciding how to implement required security controls set forth in the CJIS Security Policy. The corresponding federal controls are listed for each policy section. Description of the federal controls can be found on the NIST web site at this location:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

Please direct any questions concerning the document to the FBI CJIS ISO program using our iso@ic.fbi.gov email address.

| CSP v5.5 Area | Requirement | NIST SP 800-53 rev. 4 Control |
|--|---|--|
| CJIS Security Policy Area 1 - Information Exchange Agreements | | |
| 5.1 | Policy Area 1: Information Exchange Agreements | N/A |
| 5.1.1 | Information Exchange | AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2) |
| 5.1.1.1 | Information Handling | AC-21, CM-9, CP-6, CP-7, IR-8, PL-2, PM-1 |
| 5.1.1.2 | State and Federal Agency User Agreements | AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2) |
| 5.1.1.3 | Criminal Justice Agency User Agreements | AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2) |
| 5.1.1.4 | Inter-Agency and Management Control Agreements | AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2) |
| 5.1.1.5 | Private Contractor User Agreements and CJIS Security Addendum | AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2) |
| 5.1.1.6 | Agency User Agreements | AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2) |
| 5.1.1.7 | Outsourcing Standards for Channelers | PE-3, PS-1, PS-2, PS-3, PS-6, PS-7 |
| 5.1.1.8 | Outsourcing Standards for Non-Channelers | AC-21, CA-3, SA-2, SA-4, SA-4(1), SA-12(2) |
| 5.1.2 | Monitoring, Review, and Delivery of Services | RA-3, SA-9, SA-9(1) |
| 5.1.2.1 | Managing Changes to Service Providers | RA-3 |
| 5.1.3 | Secondary Dissemination | PS-3, PS-6, PS-7 |
| 5.1.4 | Secondary Dissemination of Non-CHRI CJI | PS-3, PS-6, PS-7 |
| CJIS Security Policy Area 2 - Security Awareness Training | | |
| 5.2 | Policy Area 2: Security Awareness Training | N/A |
| 5.2.1 | Awareness Topics | AT-1, PL-4, PL-4(1) |
| 5.2.1.1 | Level One Security Awareness Training | AT-2, AT-3 |
| 5.2.1.2 | Level Two Security Awareness Training | AT-2(2), AT-3, PL-4, PL-4(1) |
| 5.2.1.3 | Level Three Security Awareness Training | AT-2(2), AT-3, PL-4, PL-4(1) |
| 5.2.1.4 | Level Four Security Awareness Training | AT-3, CM-10 |
| 5.2.2 | Security Training Records | AT-4, PL-4 |
| CJIS Security Policy Area 3 - Incident Response | | |
| 5.3 | Policy Area 3: Incident Response | N/A |
| 5.3.1 | Reporting Information Security Events | IR-4(1), IR-6, IR-6(1), IR-6(2), IR-7, IR-7(1), IR-7(2), IR-8, PE-17 |
| 5.3.1.1.1 | FBI CJIS Division Responsibilities | N/A |
| 5.3.1.1.2 | CSA ISO Responsibilities | N/A |
| 5.3.2 | Management of Security Incidents | IR-1, IR-8 |
| 5.3.2.1 | Incident Handling | IR-4, IR-4(1), IR-4(3), IR-4(4), IR-8 |
| 5.3.2.2 | Collection of Evidence | IR-4, IR-4(1), IR-4(3), IR-4(4), IR-8 |
| 5.3.3 | Incident Response Training | IR-2, IR-3 |
| 5.3.4 | Incident Monitoring | IR-5 |

| CSP v5.5 Area | Requirement | NIST SP 800-53 rev. 4 Control |
|--|--|--|
| CJIS Security Policy Area 4 - Auditing and Accountability | | |
| 5.4 | Policy Area 4: Auditing and Accountability | N/A |
| 5.4.1 | Auditable Events and Content (Information Systems) | AC-9, AU-2, AU-2(3), AU-3, AU-3(1), AU-6, AU-6(1), AU-6(3), AU-12, CA-7 |
| 5.4.1.1 | Events | AC-9, AU-2, AU-12, CA-7 |
| 5.4.1.1.1 | Content | AU-12 |
| 5.4.2 | Response to Audit Processing Failures | AU-5, AU-5(2) |
| 5.4.3 | Audit Monitoring, Analysis, and Reporting | AU-6, AU-6(1), AU-6(3), AU-7, CA-7 |
| 5.4.4 | Time Stamps | AU-8, AU-8(1) |
| 5.4.5 | Protection of Audit Information | AU-9, AU-9(4) |
| 5.4.6 | Audit Record Retention | AU-4, AU-5(1), AU-9(2), AU-11 |
| 5.4.7 | Logging NCIC and III Transactions | AU-4, AU-11 |
| CJIS Security Policy Area 5 - Access Control | | |
| 5.5 | Policy Area 5: Access Control | N/A |
| 5.5.1 | Account Management | AC-2, AC-5, IR8 |
| 5.5.2 | Access Enforcement | AC-2, AC-2(1), AC-2(7), AC-3, AC-3(3), AC-3(4), AC-5, AC-6(1), AC-6(2), AC-12(1), SC-23(1), SC-23(3) |
| 5.5.2.1 | Least Privilege | AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5) |
| 5.5.2.2 | System Access Control | AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5) |
| 5.5.2.3 | Access Control Criteria | AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5) |
| 5.5.2.4 | Access Control Mechanisms | AC-2, AC-2(4), AC-2(7), AC-5, AC-6, AC-6(5), AC-6(9), AC-10, RA-5(5) |
| 5.5.3 | Unsuccessful Login Attempts | AC-7, IA-5(1) |
| 5.5.4 | System Use Notification | AC-8, AC-11(1), AC-22 |
| 5.5.5 | Session Lock | AC-11 |
| 5.5.6 | Remote Access | AC-17, AC-17(3), AC-17(4), AC-17(6) |
| 5.5.6.1 | Personally Owned Information Systems | AC-17 |
| 5.5.6.2 | Publicly Accessible Computers | AC-17, AC-22 |

| CSP v5.5 Area | Requirement | NIST SP 800-53 rev. 4 Control |
|--|---|--|
| CJIS Security Policy Area 6 - Identification and Authentication | | |
| 5.6 | Policy Area 6: Identification and Authentication | N/A |
| 5.6.1 | Identification Policy and Procedures | IA-1, IA-2, IA-2(5) |
| 5.6.1.1 | Use of Originating Agency Identifiers in Transactions and Information Exchanges | SC-16 |
| 5.6.2 | Authentication Policy and Procedures | IA-1, IA-2, IA-2(8), IA-2(9), IA-3 |
| 5.6.2.1 | Standard Authenticators | IA-5, IA-5(1), IA-5(5), IA-6 |
| 5.6.2.1.1 | Password | IA-5, IA-5(1), IA-5 (4) |
| 5.6.2.1.2 | Personal Identification Number (PIN) | IA-5, IA-5(1), IA-5 (4) |
| 5.6.2.2 | Advanced Authentication | IA-2(1), IA-2(2), IA-2(3),IA-2(4), IA-2(11), IA-2(13), IA-3(1), IA-5(2), IA-5(11), MA-4, SC-37, SC-37(1) |
| 5.6.2.2.1 | Advanced Authentication Policy and Rationale | IA-2(1), IA-2(2), IA-2(3),IA-2(4), IA-2(11), IA-3(1), IA-5(2), IA-5(11), MA-4 |
| 5.6.2.2.2 | Advanced Authentication Decision Tree | IA-2(1), IA-2(2), IA-2(3),IA-2(4), IA-2(11), IA-3(1), IA-5(2), IA-5(11), MA-4 |
| 5.6.3 | Identifier and Authenticator Management | IA-4, IA-4(2), IA-4(4), IA-5, IA-5(8), IA-8 |
| 5.6.3.1 | Identifier Management | AC-2(3), IA-4, IA-4(2), IA-4(4), IA-5(3), IA-5(8), IA-8 |
| 5.6.3.2 | Authenticator Management | IA-5, IA-5(6), IA-5(8) |
| 5.6.4 | Assertions | IA-2(12), IA-8(1), IA-8(2), IA-8(3) |
| CJIS Security Policy Area 7 - Configuration Management | | |
| 5.7 | Policy Area 7: Configuration Management | N/A |
| 5.7.1 | Access Restrictions for Changes | CM-3, CM-3(2), CM-4, CM-4(2), CM-5(5), CM-5(6), CM-6, CM-9, MA-2, MA-5, SA-10 |
| 5.7.1.1 | Least Functionality | CM-2, CM-3, CM-6, CM-7, CM-7(1), CM-7(2), CM-7(3), CM-7(4), CM-7(5), CM-8(3), CM-10, CM-11, SA-4(9), SA-9(2) |
| 5.7.1.2 | Network Diagram | CA-3, CA-9, SC-7(4) |
| 5.7.2 | Security of Configuration Documentation | CM-2, CM-5, CM-5(1), CM-5(2), CM-8, CM-8(1), CM-9, SA-5 |
| CJIS Security Policy Area 8 - Media Protection | | |
| 5.8 | Policy Area 8: Media Protection | N/A |
| 5.8.1 | Media Storage and Access | AC-20(2), CP-6, CP-7, MA-3(3), MP-2, MP-3, MP-4 |
| 5.8.2 | Media Transport | MP-5 |
| 5.8.2.1 | Digital Media in Transit | MP-5, MP-5(4) |
| 5.8.2.2 | Physical Media in Transit | MP-5 |
| 5.8.3 | Digital Media Sanitization and Disposal | MA-2, MP-6, MP-6(1), MP-6(2), MP-6(3) |
| 5.8.4 | Disposal of Physical Media | MP-6 |

| CSP v5.5 Area | Requirement | NIST SP 800-53 rev. 4 Control |
|---|--|---|
| CJIS Security Policy Area 9 - Physical Protection | | |
| 5.9 | Policy Area 9: Physical Protection | N/A |
| 5.9.1 | Physically Secure Location | PE-1 |
| 5.9.1.1 | Security Perimeter | PE-1 |
| 5.9.1.2 | Physical Access Authorizations | MA-4(7), MA-5, PE-2, PE-2(1) |
| 5.9.1.3 | Physical Access Control | PE-3, PE-3(3) |
| 5.9.1.4 | Access Control for Transmission Medium | PE-4 |
| 5.9.1.5 | Access Control for Display Medium | PE-5 |
| 5.9.1.6 | Monitoring Physical Access | PE-3, PE-5, PE-6, PE-6(1) |
| 5.9.1.7 | Visitor Control | PE-2(3), PE-3 |
| 5.9.1.8 | Delivery and Removal | PE-8 |
| 5.9.2 | Controlled Area | PE-2, PE-5 |
| CJIS Security Policy Area 10 - Systems and Communications Protection and Information Integrity | | |
| 5.10 | Policy Area 10: System and Communications Protection and Information Integrity | N/A |
| 5.10.1 | Information Flow Enforcement | AC-4, AC-20, AC-20(1), CA-3, CA-9, IA-5(7), SC-7(4), SC-7(8), SC-7(11), SC-10, SC-15, SC-15(1) |
| 5.10.1.1 | Boundary Protection | AC-20, CA-3(1), CA-3(2), CA-3(5), PE-3(2), SC-5, SC-5(1), SC-5(2), SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(7), SC-7(8), SC-7(11), SC-7(12), SC-7(13), SC-7(14), SC-7(18), SC-24 |
| 5.10.1.2 | Encryption | AC-17(2), IA-7, MA-4(6), SC-8, SC-8(1), SC-8(2), SC-11, SC-12, SC-12(1), SC-12(2), SC-12(3), SC-13, SC-17, SC-28, SC-28(1), SI-7(6) |
| 5.10.1.3 | Intrusion Detection Tools and Techniques | SC-7(19), SI-4, SI-4(1), SI-4(2), SI-4(4), SI-4(5), SI-4(7), SI-4(9), SI-4(11), SI-4(12), SI-7, SI-7(1), SI-7(7) |
| 5.10.1.4 | Voice over Internet Protocol | SC-19 |
| 5.10.1.5 | Cloud Computing | AC-17, AC-17(1), AC-17(2), AC-17(3), AC-17(4), AC-23, CP-1, CP-2(1), CP-2(3), CP-2(8), CP-6(1), CP-6(3), CP-7, CP-9, CP-10, CP-10(2), IA-1, IA-2, IR-1, IR-6, IR-8, IR-9, MA-1, MA-5, MA-5(4), MP-1, MP-2, MP-4, MP-5, MP-6, MP-7, MP-7(1), PE-1, PE-2, PE-3, PE-18, PL-1, PL-2, PL-2(3), PL-4, PL-4(1), PL-7, PL-8, PL-9, PS-1, PS-3, PS-7, SC-2, SC-2(1), SC-3, SC-4, SC-5, SC-5(1), SC-5(2), SC-5(3), SC-6, SC-7, SC-8, SC-9, SC-12, SC-13, SC-13 (1), SC-16, SC-16 (1), SC-20, SC-21, SC-22, SC-23, SC-28, SC-28 (1), SC-28 (2), SC-32, SC-36, SC-38, SC-43, SI-1 |
| 5.10.2 | Facsimile Transmission of CJI | N/A |
| 5.10.3 | Partitioning and Virtualization | SC-2, SC-4 |
| 5.10.3.1 | Partitioning | SC-2, SC-2(1), SC-3, SC-4, SC-32 |
| 5.10.3.2 | Virtualization | SC-2, SC-4 |
| 5.10.4 | System and Information Integrity Policy and Procedures | N/A |

| CSP v5.5 Area | Requirement | NIST SP 800-53 rev. 4 Control |
|--|--|---|
| 5.10.4.1 | Patch Management | CM-3, CM-4, CM-4(1), RA-5, RA-5(1), RA-5(2), RA-5(3), SA-11, SA-11(1), SI-2, SI-2(2), SI-2(3) |
| 5.10.4.2 | Malicious Code Protection | MA-3(2), SI-3, SI-3(1), SI-3(2) |
| 5.10.4.3 | Spam and Spyware Protection | SI-8, SI-8(1), SI-8(2) |
| 5.10.4.4 | Security Alerts and Advisories | SI-5, SI-5(1), SI-11 |
| 5.10.4.5 | Information Input Restrictions | SI-10, SI-12 |
| CJIS Security Policy Area 11 - Formal Audits | | |
| 5.11 | Policy Area 11: Formal Audits | N/A |
| 5.11.1 | Audits by the FBI CJIS Division | N/A |
| 5.11.1.1 | Triennial Compliance Audits by the FBI CJIS Division | CA-2, CA-7 |
| 5.11.1.2 | Triennial Security Audits by the FBI CJIS Division | CA-2 |
| 5.11.2 | Audits by the CSA | CA-2 |
| 5.11.3 | Special Security Inquiries and Audits | CA-2(1), CA-3, CA-5, CA-6, CA-7(1), CM-3(4) |
| CJIS Security Policy Area 12 - Personnel Security | | |
| 5.12 | Policy Area 12: Personnel Security | N/A |
| 5.12.1 | Personnel Security Policy and Procedures | N/A |
| 5.12.1.1 | Minimum Screening Requirements for Individuals Requiring Access to CJI | PS-2, PS-3, PS-3(1), PS-3(2), PS-3(3), PS-6, PS-6(2), PS-7 |
| 5.12.1.2 | Personnel Screening for Contractors and Vendors | PS-2, PS-3, PS-7 |
| 5.12.2 | Personnel Termination | PS-4 |
| 5.12.3 | Personnel Transfer | PS-5 |
| 5.12.4 | Personnel Sanctions | PS-8 |

| CSP v5.5 Area | Requirement | NIST SP 800-53 rev. 4 Control |
|--|---|---|
| CJIS Security Policy Area 13 - Mobile Devices | | |
| 5.13 | Policy Area 13: Mobile Devices | N/A |
| 5.13.1 | Wireless Communications Technologies | AC-18, SI-4(14), SI-4(15) |
| 5.13.1.1 | 802.11 Wireless Protocols | AC-18(5), SI-4(15) |
| 5.13.1.2 | Cellular Devices | AC-19, AC-19(5) |
| 5.13.1.2.1 | Cellular Service Abroad | AC-19, AC-19(5) |
| 5.13.1.2.2 | Voice Transmissions Over Cellular Devices | AC-19, AC-19(5) |
| 5.13.1.3 | Bluetooth | AC-18(5) |
| 5.13.1.4 | Mobile Hotspots | AC-18, AC-18(1), AC-19, IA-5, IA-5(1), IA-5 (4), SC-40, SI-4(14), SI-4(15) |
| 5.13.2 | Mobile Device Management (MDM) | AC-19, AC-19(5) |
| 5.13.3 | Wireless Device Risk Management | AC-19, AC-19(5) |
| 5.13.4 | System Integrity | CM-1, CM-2, CM-2(1), CM-2(3), CM-2(7), CM-3, CM-3(1), CM-3(2) |
| 5.13.4.1 | Patching/Updates | CM-3, CM-4, CM-4(1), RA-5, RA-5(1), RA-5(2), RA-5(3), SA-11, SA-11(1), SI-2, SI-2(2), SI-2(3) |
| 5.13.4.2 | Malicious Code Protection | MA-3(2), SI-3, SI-3(1), SI-3(2) |
| 5.13.4.3 | Personal Firewall | SC-18, SC-18(1), SC-18(2), SC-18(3), SC-18(4) |
| 5.13.5 | Incident Response | IR-1, IR-2, IR-4, IR-8 |
| 5.13.6 | Access Control | AC-5, AC-6, AC-6(5), AC-6(9), AC-19, AC-19(5) |
| 5.13.7 | Identification and Authentication | IA-1, IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(8), IA-2(9), IA-2(11), IA-3, IA-5(2), IA-5(11), MA-4, SC-37, SC-37 (1) |
| 5.13.7.1 | Local Device Authentication | IA-1, IA-2, IA-2(5) |
| 5.13.7.2 | Advanced Authentication | IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(11), IA-2(13), IA-3(1), IA-5(2), IA-5(11), MA-4, SC-37, SC-37(1) |
| 5.13.7.2.1 | Compensating Controls | AC-19, IA-3, IA-3(4), PE-18, PE-18(1), PE-20 |
| 5.13.7.3 | Device Certificates | AC-19, IA-3, IA-3(4) |