A Guide to FBI CJIS Security Policy

For our nation's leading criminal justice database

What it is

Things to Know

Key Issue

Tools for Success

Welcome to the leading database for justice

The Criminal Justice Information and Services division of the FBI, known as CJIS (pronounced See-Jis), serves as a central repository for the bureau's massive amount of criminal data and as an access portal for the agency's multiple services. Its mission is to help equip agencies with up-to-date criminal justice information (CJI) to better serve their community. It includes:

- Integrated Automated Fingerprint Identification System (IAFIS)
- National Crime Information Center (NCIC)
- Uniform Crime Reporting (UCR) Program
- Next Generation Identification (NGI)
- National Data Exchange (N-DEx)
- Enforcement Enterprise Portal (LEEP)
- Nation Instant Criminal Background Check System (NICS).

The CJIS security policy was created to provide controls to protect the full lifecycle of CJI, whether at rest or in transit. It provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI.

The policy integrates guidance from the National Institute of Standards and Technology (NIST) for a unified cybersecurity framework. This leverages existing best practices to simplify operations, increase efficiency, and speed processes.To read the full CJIS security policy, please visit: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

© 2020 Cisco and/or its affiliates. All rights reserved.

Key things to know

Since Criminal Justice Information (CJI) is extremely sensitive (biometric data, identity history, biographic, property data, and case histories), the FBI enforces three important things:

- Security Requirements – your agency must meet all minimum security requirements to keep access to CJIS
- Access Compliance – everyone (contractors, private entities, non-justice reps, justice reps) that handles or supports CJIS information must fully comply with 13 security policy areas
- Audits – your agency must pass an FBI directed audit every three years.

Deeper dive:

Thirteen security policy areas to guide your security

To help you better understand each security policy area, we've created the quick-reference graph to the right. Plus we've listed the solutions that can help make your agency's compliance much easier.

How CJIS security policies help you

- The CJIS security policy provides a secure framework of laws, standards, and elements of published and vetted policies
- Supplies security requirements, guidelines and agreements, based on the will of Law Enforcement and criminal justice agencies, that protect CJI
- Provides appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit

CJIS security policy	How it adds value	Where Cisco can help
1 Information Exchange Agreements	Makes sure everyone sharing info agrees to same security standards.	-
2 Security Awareness Training	Sets your regular training schedules.	-
3 Incident Response	Protects your agency with deep network visibility, faster threat detection, advanced malware protection, and threat analytics backed by advanced machine learning.	Firepower Stealthwatch Umbrella Dashboard/Investigate Web/email Security Dashboards Cognitive Threat Analytics ISE
4 Auditing and Accountability	Provides device profiling, highly secure access control and easy onboarding.	Identity Services Engine (ISE)
5 Access Control	Enables firewall, antivirus, intrusion prevention, device profiling and VPN capabilities to keep access secure. Provides greater network visibility and faster threat detection across popular PC/mobile devices.	Router/Switch Access Lists ASA Firewall Firepower Threat Defense Identity Services Engine Wireless LAN Controller/Access AnyConnect VPN
6 Identification and Authentication	Makes sure only authorized devices and personnel gain entry into CJIS from your network thru secure access control faster threat detection.	LAN Switches/802.1x Wireless LAN Controller Identity Services Engine AnyConnect VPN
7 Configuration Management	Prevent unwanted changes to network.	Identity Security Solutions (ISE)
8 Media Protection	Unifies VPN ecosystem, keeps access to digital/physical media, in all forms, restricted to authorized individuals only.	AnyConnect VPN Flex VPN / GET VPN MACsec
9 Physical Protection	Easily configure, manage, display and control IP video network to keep your facility safe/GIS compatible.	Video Surveillance Manager (VSM) IP Surveillance Cameras
10 System/Communication Protection	Threat-centric security keeps network safe across entire attack continuum.	Cisco security solution portfolio (non-compliant cloud excluded)
11 Formal Audits	Ensures your agency stays on target	-
12 Personnel Security	Maintains integrity of your personnel	-
13 Mobile Devices	Sets device profiling, highly secure access control and easy onboarding w/greater network visibility and faster threat detection via advanced analysis and investigation across devices.	Identity Services Engine AnyConnect VPN Wireless LAN Controller and Access Points AMP for Endpoints

© 2020 Cisco and/or its affiliates. All rights reserved.

Key issue

What if Your Agency Fails an Audit?

Did you know that failure to pass the required CJIS Security Policy audit could:

- Terminate your agency's access to CJIS if the issues uncovered are not corrected
- Damage your agency's reputation and working relationships in the community
- Raise concerns about your agency's ability to follow procedures critical to successful case prosecutions.

Fortunately, Cisco can help you achieve compliance before an audit takes place. But if your agency has failed an audit, we can also help by matching you with the right technology-based solutions to correct it.

Next steps

To learn more about solutions to help you comply with FBI CJIS mandates, visit:
Cisco Cybersecurity for Government

© 2020 Cisco and/or its affiliates. All rights reserved.

How your agency can comply with FBI CJIS security policy

Strategically manage your agency's risk

Agencies like yours are facing a growing wave of cyber threats. These can include:

- Ransomware and phishing scams
- Insider theft of data and manipulation
- Coordinated hacks
- Unauthorized access via stolen devices.

The good news is that Cisco has spent years partnering with government agencies to create solutions based on NIST standards as well as:

- Media Access Control Security (MACsec) and secure VPNs for authenticating and encrypting packets
- A holistic security approach the provides deeper visibility into your network and endpoints attaching to it.
- Federal Information Processing Standard (FIPS140-2) Federal encryption standard.

Seek simple and secure solutions

Our industry-leading solutions, combined with our deep working knowledge of CJIS, helps your agency to comply with the following security policy (SP) areas:

- SP3: Solutions for Incident Response

  Our solutions can help protect your agency by adding deep network visibility, faster threat detection, malware protection, and threat analytics backed by advanced machine learning.

  We make compliance easier with industry-leading solutions like Firepower, Stealthwatch and ISE.
- SP5: Solutions for Access Control

  Cisco can help enable firewall, antivirus, intrusion prevention, device profiling and VPN capabilities that keep your access secure while providing greater network visibility and faster threat detection across mobile devices.

  By deploying ASA Firewall, Firepower Threat Defense, ISE, and Wireless LAN Controller/Access you can secure access.
- SP8: Solutions for Media Protection

  We lead the industry with encryption solutions that are FIPS140-2 certified (critical to meet CJIS Security Policy). AnyConnect VPN, Flex VPN and MACsec you can unify your VPN ecosystem and restrict access to digital/physical media, in all forms, to authorized individuals only.
- SP10: Solutions for System/Communications Protection

  Cisco's unrivaled end-to-end security portfolio can address your CJIS technology concerns. Our industry-leading cybersecurity solutions provide a threat-centric approach the empowers you with greater insight into emerging threat landscapes.
- SP13: Solutions for Mobile Devices

  With Cisco ISE, AnyConnect VPN, AMP for Endpoints, and other industry-leading solutions, you gain control of device profiling, greater network visibility and faster threat detection via advanced analysis and investigation for a variety of mobile devices.