CJIS SECURITY POLICY EVALUATION GUIDE

AVOID COMPLIANCE ISSUES AND ENSURE UNINTERRUPTED ACCESS TO CJI

CJIS wants you to prove that devices are encrypted and you could remotely wipe them. I was really impressed with Absolute's ability to see any device, check its status, and remotely freeze or wipe it, as long as it has any kind of internet connection, even if all other security has been removed.

COREY NELSON, IT MANAGER
EMERGENCY COMMUNICATIONS OF SOUTHERN OREGON

The public relies on law enforcement and justice departments to protect us from crime. To execute on this promise safely and efficiently, timely and secure access to data is required.

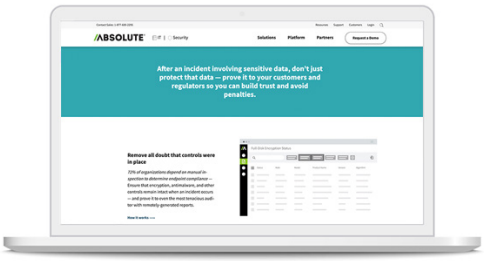
The Criminal Justice Information Services (CJIS) Division of the FBI equips law enforcement, national security, civil agencies, and intelligence community partners with the criminal justice information (CJI) they need, including (but not limited to): biometric, identity history, biographic, property, and case/incident history data.

THE CJIS SECURITY POLICY

The CJIS Security Policy establishes the **minimum security controls required to grant agencies access to CJIS systems and information**, in order to protect the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI. Each agency is encouraged to implement additional controls to address its specific risks.

These controls affect several areas:

1. Inventory and audits
2. Access control and data protection
3. Endpoint security controls
4. Risk and incident response



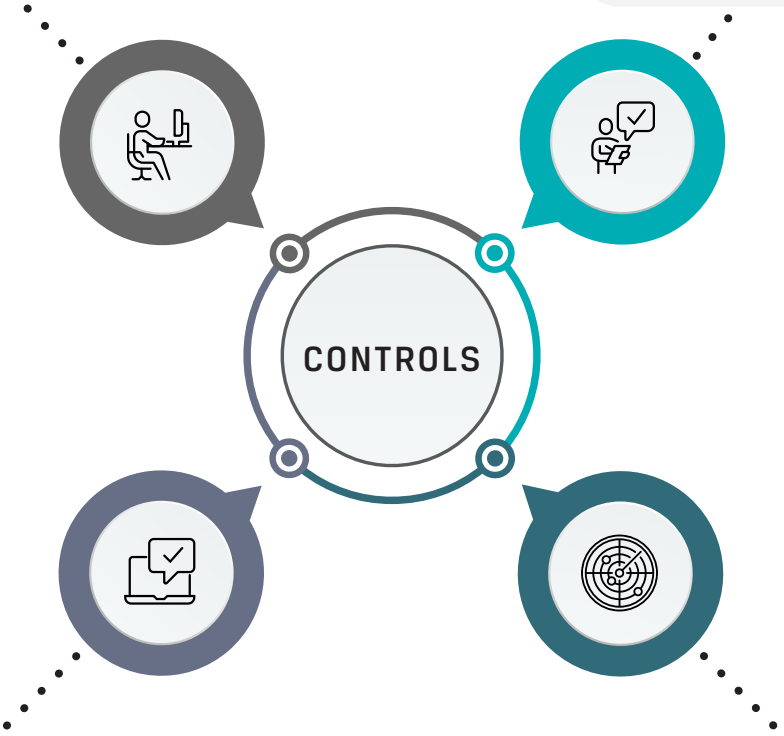
Learn more about how to prove compliance with Absolute: absolute.com/compliance

RISK AND INCIDENT RESPONSE

- CJIS Policy Area 3. Incident Response
- CJIS Policy Area 13. Mobile Devices (Risk & Response)

INVENTORY AND AUDITS

- CJIS Policy Area 4. Audit and Accountability
- CJIS Policy Area 7. Configuration Management
- CJIS Policy Area 11. Formal Audits



ENDPOINT SECURITY CONTROLS

- CJIS Policy Area 10. Systems and Communications Protection and Information Integrity
- CJIS Policy Area 13. Mobile Devices (Security Controls)

ACCESS CONTROL AND DATA PROTECTION

- CJIS Policy Area 5. Access Control
- CJIS Policy Area 6. Identification and Authentication
- CJIS Policy Area 8. Media Protection
- CJIS Policy Area 9. Physical Protection
- CJIS Policy Area 12. Personnel Security

CJIS COMPLIANCE ACROSS AN ENDPOINT POPULATION

The Absolute platform delivers a comprehensive suite of capabilities for ensuring compliance with the CJIS Security Policy:

INVENTORY AND AUDITS	ABSOLUTE CAPABILITY
CJIS Policy Area 4. Audit and Accountability • Automate inventory management and audits • Keep historical logs of device activity • Generate audit records for specific device events • Generate time stamps for audit records	/A

INVENTORY AND AUDITS	ABSOLUTE CAPABILITY
CJIS Policy Area 7. Configuration Management • Discover allegedly decommissioned devices that are still active and accessing your network • Detect and document changes to configurations, hardware or software components	/A
CJIS Policy Area 11. Formal Audits • Automate and accelerate audits with ongoing compliance checks • Execute query commands on endpoints, on-demand and/or at-scale	/A

ACCESS CONTROL AND DATA PROTECTION	ABSOLUTE CAPABILITY
CJIS Policy Area 5. Access Control • Identify PII/CJI/CHRI information on endpoints, on or off network • Monitor the existence and health of encryption on any endpoint accessing CJIS systems • Remotely monitor changes to devices or components • Remotely monitor altered or removed applications • Remotely execute workflows on endpoints to remove or disable user accounts • Monitor network or physical location of devices, on or off network • Integrate with Microsoft AIP to enable data protection that travels with the file • Remotely delete data or freeze device, on or off network • Remotely disable USB ports on endpoints, on or off network	/A
CJIS Policy Area 6. Identification and Authentication • Remotely remove or disable unauthorized user accounts on any endpoint, at any time	/A
CJIS Policy Area 8. Media Protection • Monitor, and restore if necessary, full-disk encryption on devices accessing CJIS systems, on or off network • Detect removal of drives from devices accessing CJIS systems • Secure and remote data delete or device wipe on endpoints, on or off network	/A
CJIS Policy Area 9. Physical Protection • Monitor device geolocation and network location • Enable geofences and automated alerts when devices leave or enter an unauthorized area	/A
CJIS Policy Area 12. Personnel Security • Remotely freeze or wipe devices as part of the normal personnel transition or termination procedure • Remotely disable or remove user accounts to prevent further access to data • Remotely freeze, isolate, or limit connectivity or functionality for personnel failing to comply with security policies	/A

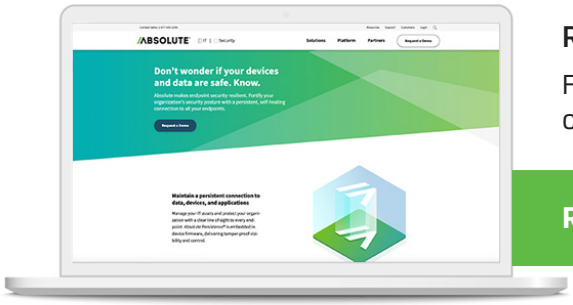
ENDPOINT SECURITY CONTROLS	ABSOLUTE CAPABILITY
CJIS Policy Area 10. Systems and Communications Protection and Information Integrity • Verify that endpoints are appropriately updated or patched • Validate and remediate device configurations • Push updates to any endpoint, at any time • Monitor, validate and restore encryption for all PII/CJI/CHRI data at rest on all devices – on or off network • Monitor and restore if necessary any critical applications on endpoints (e.g. anti-malware, SCCM/endpoint management, DLP, VPN, etc.) • Detect endpoint vulnerabilities on-demand and at-scale • Detect and remove unauthorized software applications on endpoints • Allow only authorized communication between systems • Detect cloud storage application instances on endpoints • Detect suspicious endpoint activity and remotely disable ports, or stop processes, services or applications	/A
CJIS Policy Area 13. Mobile Devices (Security Controls) • Validate and remediate appropriate device configurations • Monitor device geolocation, including historical logs • Detect unpatched and vulnerable devices • Monitor encryption and anti-malware status • Detect and remove unauthorized apps on devices, e.g. cloud storage	/A

RISK AND INCIDENT RESPONSE	ABSOLUTE CAPABILITY
CJIS Policy Area 3. Incident Response • Detect early precursors to security incidents • Automatic reports and historical logs of endpoint activity/events • Query any endpoint on or off the network for deep visibility and proof of compliance • Provide proof that controls were intact at the time of the incident • Contain/isolate/freeze device, on or off network • Leverage a team of experienced investigators with access to forensic tools • Interface with your departmental incident handling systems through our API	/A
CJIS Policy Area 13. Mobile Devices (Risk and Incident Response) • Detect use of unauthorized USB storage • Remotely freeze devices • Remotely wipe data on devices • Assess device risk or investigate incidents in depth	/A

TAKEAWAYS

Combating cybersecurity risks and complying with the stringent compliance requirements of the CJIS Security Policy are vital for today's law enforcement and justice departments. IT and Information Security teams need to be equipped with powerful, versatile tools that will allow them to increase their operational efficiency.

Government agencies turn to Absolute for persistent endpoint visibility and control. Absolute helps protect regulated data, eliminate compliance failures, and respond rapidly to security exposures. Uninterrupted access to CJIS data means business continuity and the ability to ensure field staff productivity and safety. Always.



REQUEST A DEMO

Find out how our solutions can benefit your organization.

REQUEST DEMO

ABOUT ABSOLUTE

Absolute empowers more than 12,000 customers worldwide to protect devices, data, applications and users against theft or attack—both on and off the corporate network. With the industry's only tamper-proof endpoint visibility and control solution, Absolute allows IT to enforce asset management, endpoint security, and data compliance for today's remote digital workforces. Patented Absolute Persistence™ is embedded in the firmware of Dell, HP, Lenovo, and 26 other manufacturers' devices for vendor-agnostic coverage, tamper-proof resilience, and ease of deployment.

EMAIL:
sales@absolute.com

SALES:
absolute.com/request-a-demo

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

WEBSITE:
absolute.com