RAPID7

SOLUTION BRIEF

SUPPORTING CJIS COMPLIANCE WITH RAPID7

Utilizing Rapid7 Solutions to Secure CJI and Ensure Compliance

The Criminal Justice Information Services (CJIS) Security Policy is a comprehensive set of standards designed to safeguard Criminal Justice Information (CJI) from unauthorized access, disclosure, and compromise. It establishes a series of security controls across key areas such as data storage, access control, incident response, and system monitoring, with the goal of ensuring that sensitive criminal justice data remains protected at all times.

However, achieving CJIS compliance can be a challenging and resource-intensive task for many organizations due to the lack of a centralized authority or standardized assessment framework. Rapid7 simplifies this process by providing robust solutions and services that are specifically designed to align with key CJIS controls, helping organizations meet the complex requirements for protecting CJI and reducing overall compliance risk.

CJIS Control Areas and Rapid7 Solutions

- **Data Storage and Protection**
  Customers may select the United States as their data storage location and, if chosen, Rapid7 ensures that all customer data remains in the United States, fully adhering to CJIS's requirement for localized data storage. While Rapid7 limits the collection of Personally Identifiable Information (PII) where possible, it implements robust security and compliance measures to protect customer data and reduce regulatory complexity.

- **Vulnerability Management**
  Through InsightVM, Rapid7 continuously identifies, assesses, and remediates vulnerabilities across systems. This approach ensures that systems processing or storing CJI remain secure and up to date, addressing the CJIS configuration management requirements effectively.

- **Threat Detection and Incident Response**
  Rapid7's InsightIDR and Managed Detection and Response (MDR) services provide advanced capabilities in detecting and investigating suspicious activities. By leveraging User Behavior Analytics (UBA), these solutions offer 24/7 monitoring, as well as expert incident response assistance. This helps meet CJIS requirements for incident detection, response, and mitigation.

- **Auditing and Accountability**
  InsightIDR offers robust auditing capabilities, tracking system access, user activities, and administrative actions. This creates a clear audit trail to demonstrate compliance, ensuring that only authorized personnel can access CJI and that all access is thoroughly documented.

- **Access Control and Authentication**
  Rapid7's InsightIDR integrates with Identity and Access Management (IAM) solutions to provide multi-factor authentication (MFA) and role-based access control. These capabilities help secure access to CJI, reducing the risk of unauthorized activities in line with CJIS standards.

- **Security Awareness Training**
  Rapid7 enhances security awareness by leveraging its open-source research and threat intelligence. Through projects such as Metasploit and regular publications on emerging cyber threats, Rapid7 empowers organizations with actionable insights to stay ahead of evolving security risks. This ongoing resource contribution helps meet CJIS's requirements for security awareness training.

- **Cloud Security**
  InsightCloudSec delivers continuous security and compliance monitoring for cloud environments. The solution automates the remediation of misconfigurations, ensuring cloud assets are aligned with CJIS policy requirements. By providing visibility into cloud workloads, it helps identify potential risks to CJI and ensures compliance in dynamic cloud environments.

- **Surface Monitoring**
  Rapid7's Surface Command provides real-time visibility into external attack surfaces, enabling organizations to identify vulnerabilities and misconfigurations before they can be exploited. By monitoring domains, IPs, and digital assets, the solution detects potential threats and alerts organizations to risks associated with exposed assets or sensitive information. This enhances situational awareness and allows for proactive management of external threats to CJI.

- **Incident Readiness and Response**
  Rapid7's Incident Response (IR) Services prepare organizations to handle security incidents, from proactive planning to real-time support. We develop customized response plans, conduct simulated exercises, and train teams for quick action. During active incidents, our experts assist with containment, eradication, and recovery, minimizing impact and ensuring compliance with CJIS requirements.

- **Government Partnerships**
  Rapid7 has a proven track record of working with government agencies, including state Departments of Corrections. This demonstrates the company's expertise in CJIS-regulated environments, offering tailored solutions to meet the unique needs of law enforcement and criminal justice organizations.

Securing Your Path to Compliance

Achieving CJIS compliance can be a complex process, but Rapid7 simplifies this journey by providing solutions and expertise aligned with CJIS Security Policy controls. From secure data storage to advanced threat detection, auditing, and training, Rapid7 equips organizations with the tools and resources necessary to protect CJI and maintain compliance.

Note: For updated guidance and sanctionable requirements under Priority 1, refer to the changes effective since October 2024, as outlined in the FBI's updated Criminal Justice Information Services (CJIS) Security Policy. See Wilson Elser's publication on the topic: "FBI Has Updated the Criminal Justice Information Services (CJIS) Security Policy," available at https://www.wilsonelser.com/publications/fbi-has-updated-the-criminal-justice-information-services-cjis-security-policy.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit:
rapid7.com/try/insight