carahsoft

TANIUM | Public Sector

Achieve CJIS V6.0 Compliance with Tanium

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP V, CMAS and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Tanium, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/taniumresources

Join Events & Webinars:
carah.io/taniumevents

Discover Technology Solutions:
carah.io/tanium

Learn About Procurement:
carah.io/taniumcontracts

Connect With Our Team:
Tanium@carahsoft.com
(703)673-3560

TANIUM

WHITEPAPER

Achieve CJIS V6.0 Compliance with Tanium

Operationalizing real-time endpoint visibility, automated control and defensible audit readiness for criminal justice information.

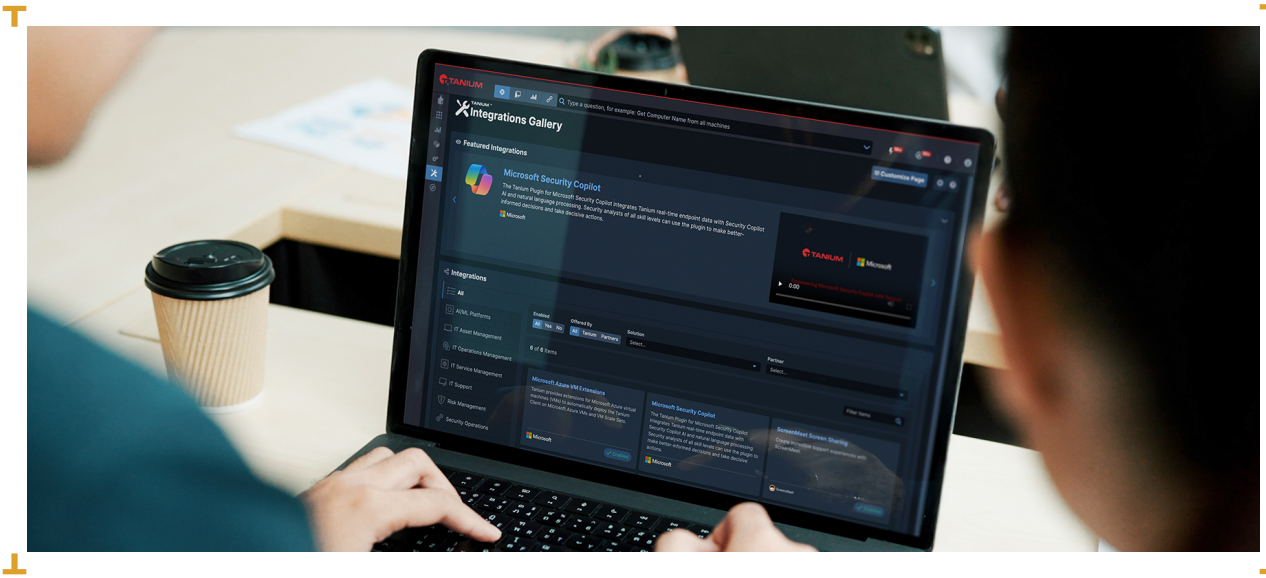
Why does this matter now?

The stakes for U.S. law enforcement and justice organizations have never been higher. Ransomware, supply chain compromises, credential abuse, and rapidly evolving cyber threats continue to target agencies responsible for safeguarding Criminal Justice Information (CJI). To meet this escalating risk, the Federal Bureau of Investigation (FBI) has released Criminal Justice Information Services (CJIS) Security Policy v6.0, a transformative update that shifts agencies away from static, checklist-driven compliance and toward a model of continuous security, real-time monitoring, and modernized defense aligned with NIST-based cybersecurity frameworks.

CJIS v6.0 represents a major evolution in how agencies are expected to protect the systems and data that underpin justice operations. The policy introduces stronger requirements for identity controls, asset management, incident response, and operational resilience, raising expectations for visibility, accountability, and security across every environment handling CJI. Updated control families—including Assessment, Authorization & Monitoring; Personnel Security; System & Services Acquisition; and Supply Chain Risk Management—reflect today's threat landscape and empower agencies to focus resources where they matter most.

With the launch of the "CJIS v6.0 "Zero Cycle Window" (Oct. 1, 2024 – Sept. 30, 2027), agencies now have a defined period to interpret, operationalize, and begin implementing the new requirements before they become fully enforceable in audits. This phase marks a pivotal transition from planning to action. Agencies that begin modernization efforts now will be best positioned for compliance and resilience as enforcement ramps up.

Adopting CJIS v6.0 is more than a regulatory necessity—it is an investment in public trust and the operational integrity of the justice system. Strengthening controls, modernizing security practices, and embracing continuous monitoring ensure that agencies can operate securely, efficiently, and confidently despite an increasingly hostile cyber environment. The updated policy reinforces that CJIS security is a shared responsibility: both agencies and their service providers must uphold these enhanced protections to sustain a resilient, trustworthy, and compliant ecosystem.



Tanium Autonomous IT Platform:

Powering CJIS v6.0 enablement across five strategic categories

The Tanium Autonomous IT Platform delivers the real-time endpoint intelligence, control, and automation required to operationalize CJIS v6.0 across its five strategic security categories. By converging endpoint management, security operations, exposure management, and compliance into a single-agent, single-platform architecture, Tanium provides continuous configuration enforcement, autonomous remediation, and authoritative telemetry across every device handling Criminal Justice Information (CJI). This unified operational model directly supports CJIS v6.0's shift toward continuous monitoring, matured identity and access controls, enhanced supply chain assurances, and evidence-backed compliance—reducing audit friction, increasing operational resilience, and enabling faster, data-driven decision-making across justice environments.

As CJIS v6.0 raises the standard for protecting CJI, Tanium empowers agencies with the real-time visibility and enforcement capabilities required to meet those expectations at scale—regardless of environment size, distribution, or complexity. By automating routine IT and security workflows, surfacing live endpoint state, and orchestrating rapid, repeatable response actions, the platform enables agencies to stay ahead of emerging threats, streamline compliance execution, and ensure uninterrupted mission delivery. Tanium's Autonomous IT Platform provides the clarity, control, and continuity agencies need to uphold CJIS v6.0 requirements and maintain a secure, trusted, and resilient operational ecosystem

CJIS V6.0 STRATEGIC PILLARS	PILLAR OBJECTIVE	EXAMPLE TANIUM SUPPORT
Governance & Risk Management	Ensures continuous, evidence-based governance and risk management by requiring ongoing oversight, clearly defined security roles, and continuous monitoring rather than point-in-time compliance	With real-time endpoint intelligence, automated remediation, and integrated evidence generation, Tanium strengthens strategic planning, supports ongoing risk assessments, embeds security into acquisition decisions, and enhances oversight of vendors and third-party systems
Access & Identity Management	Enforces strong identity proofing and MFA, ensuring only verified, least-privileged users can access CJI with full logging and auditability	The Tanium Autonomous IT Platform arms agencies with endpoint management, automated compliance checks, and rapid remediation that will elevate access governance, enable strong authentication practices, and assist in mitigating personnel related risks.
System & Data Protection	Implements controls to secure CJI throughout its lifecycle—at rest, in transit, and during exchange—using updated encryption, secure configurations, and protected system connections	Through unified policy execution, rapid remediation, and granular control over data movement, system configurations, and maintenance activities, Tanium strengthens communication safeguards, protects sensitive media, supports secure operational environments, and ensures maintenance actions are monitored and governed at scale.
Monitoring & Incident Response	Requires continuous monitoring, rapid detection of suspicious activity, and formal incident response processes to contain threats and maintain real time security assurance	By enabling proactive threat hunting, endpoint quarantine, rapid remediation, and the packaging and retention of detailed forensic data, Tanium streamlines CJIS-aligned auditing, strengthens incident response workflows, and ensures evidence ready visibility.
Operational Resilience	Strengthens resilience through ongoing risk assessment, supply chain oversight, and continuous governance to ensure agencies can sustain secure operations amid evolving threats	Tanium provides rapid, scalable endpoint provisioning, re-baselining, and restoration to maintain CJIS compliant configurations during incidents. Automated deployment, real time configuration enforcement, software supply chain visibility, and integrated remediation workflows ensure endpoints return to approved states quickly, reducing operational risk and preserving CJI service continuity.

Why Tanium for CJIS v6.0?

Tanium's autonomous IT capabilities are uniquely positioned to support agencies as they operationalize CJIS v6.0 through a unified, real-time platform that strengthens audit readiness, enhances operational resilience, and simplifies compliance across CJIS-relevant control families. With continuous endpoint visibility, automated evidence collection, and rapid remediation at scale, agencies can reduce audit friction, enforce secure configurations with confidence, and respond in real time to evolving threats.

Operational outcomes for CJIS-Regulated agencies

By operationalizing CJIS v6.0 through continuous visibility, control, and remediation, Tanium delivers measurable outcomes that extend beyond audit compliance:

- Reduced Compliance Risk: Continuous monitoring and automated enforcement shrink exposure windows and reduce reliance on manual, point-in-time assessments.
- Audit-Ready Assurance: Real-time telemetry and automated evidence generation provide defensible, traceable proof of control execution across CJIS domains.
- Improved Incident Readiness and Response: Live endpoint visibility, rapid containment, and forensic data collection enable faster, more effective response to security events involving CJI.
- Operational Resilience at Scale: Automated re-baselining and recovery workflows help agencies maintain CJIS-aligned configurations during incidents and disruption.
- Sustained Trust and Accountability: By strengthening governance, oversight, and system integrity, agencies reinforce public trust in the systems that support justice operations.

Conclusion

CJIS Security Policy v6.0 represents a shift toward continuous security, accountability, and resilience in the protection of Criminal Justice Information. The Tanium Autonomous IT Platform helps agencies operationalize CJIS v6.0 through real time endpoint visibility, automated control, and defensible audit readiness in an evolving threat landscape.

CJIS Security Policy v6.0 marks a decisive shift from periodic, checklist driven compliance to continuous security, operational accountability, and system wide resilience in the protection of CJI. As agencies navigate accelerating threats, heightened oversight expectations, and the demands of the v6.0 Zero Cycle transition, Tanium provides the real time endpoint visibility, automated control, and defensible audit evidence required to achieve and sustain compliance at scale. By unifying endpoint management and security leveraging AI, real-time intelligence, and autonomous actions in a single platform, Tanium enables agencies to modernize their security posture, eliminate blind spots, and uphold the integrity, availability, and resilience of justice operations in an increasingly complex threat landscape.