# CJIS v6.0 Compliance Guide

CoreReconOS | FBI CJIS v6.0 Auditing — Effective October 1, 2025

## Texas Municipal Threat Context

22 Texas municipalities were struck by a coordinated ransomware campaign in late 2025, prompting a collective $2.5M ransom demand refused by all targets. FBI CJIS v6.0 auditing went live October 1, 2025. Full compliance deadline: October 1, 2027. Every Texas municipality on Wave 1 and Wave 2 outreach lists (Mission, Borger, Fort Bend, Travis, El Paso, Comal, Round Rock, Hays, Brazoria) is now in active audit scope. A failed CJIS audit means loss of NCIC access, federal funding risk, and public exposure of criminal justice data.

## 13 CJIS Security Policy Areas — Auditor Checklist

### 1. Information Exchange
Auditors look for: Encrypted CJI transmission, written MOUs between agencies, authorization protocols before sharing
Common gaps: Unencrypted email for criminal justice data, missing MOUs with third-party vendors
CoreReconOS coverage: Sentinel — Encrypted CJI handling, MOU automation, access controls

### 2. Security Awareness Training
Auditors look for: All personnel with CJIS access complete annual security training, records on file
Common gaps: Training completed but no documentation, incomplete annual refreshers, contractor training gaps
CoreReconOS coverage: Sentinel — Annual training programs, documentation management, automated reminders

### 3. Incident Response
Auditors look for: Documented IR plan, 24/7 response capability, incident logging, reporting to TX DPS
Common gaps: No formal IR plan, response times undocumented, no TX DPS reporting mechanism
CoreReconOS coverage: Command — 24/7 SOC, 30-min response SLA, incident documentation, TX DPS coordination

### 4. Auditing & Accountability
Auditors look for: 90-day minimum audit log retention, user-level accountability, monthly review process
Common gaps: Insufficient log retention, no user-level audit trails, logs not reviewed monthly
CoreReconOS coverage: Sentinel — Automated log retention, user activity tracking, monthly compliance reports

### 5. Access Control
Auditors look for: Role-based access, least-privilege principle, background checks before CJIS access
Common gaps: Overly broad access permissions, no formal role assignments, background checks not completed
CoreReconOS coverage: Sentinel — RBAC implementation, least-privilege enforcement, background check tracking

### 6. Identification & Authentication
Auditors look for: Unique user IDs, multi-factor authentication for remote access, password standards
Common gaps: Shared accounts, no MFA for remote CJIS access, weak password policies
CoreReconOS coverage: Sentinel — Unique ID enforcement, MFA deployment, password policy automation

### 7. Configuration Management
Auditors look for: Documented baseline configurations, change management process, approval workflow
Common gaps: No formal baseline documentation, ad-hoc changes without approval, no CMDB
CoreReconOS coverage: Fortress — Configuration management database, change approval workflow, baseline documentation

### 8. Media Protection
Auditors look for: Encrypted media containing CJI, physical destruction certification, media accountability logs
Common gaps: Unencrypted USB/storage devices, no destruction certificates, media not tracked
CoreReconOS coverage: Sentinel — Media encryption, chain-of-custody logging, certified destruction procedures

### 9. Physical Protection
Auditors look for: Controlled facility access, visitor logs, CJIS data isolated in locked areas
Common gaps: No badge access controls, visitor logging incomplete, CJI data on workstations in open areas
CoreReconOS coverage: Sentinel — Physical security assessment, badge access systems, workstation security standards

### 10. Systems & Communications Protection

Auditors look for: Firewall configurations, intrusion detection, VPN for remote access to CJI systems
Common gaps: No IDS/IPS, firewall rules not documented, remote access without VPN
CoreReconOS coverage: Fortress — Firewall management, IDS/IPS, VPN enforcement, perimeter security

### 11. Formal Audits

Auditors look for: Annual self-assessments against CJIS policy, corrective action plans, evidence packages
Common gaps: No self-assessment completed, findings not tracked to closure, no audit-ready documentation
CoreReconOS coverage: Command — Annual CJIS audits, corrective action planning, audit evidence packages

### 12. Personnel Security

Auditors look for: Background reinvestigation every 5 years, termination checklists, access revocation within 24 hours
Common gaps: No reinvestigation schedule, access not revoked on termination, personnel files incomplete
CoreReconOS coverage: Sentinel — Background reinvestigation tracking, termination checklists, automated access revocation

### 13. Mobile Devices

Auditors look for: MDM with encryption, remote wipe capability, mobile device policy, GPS tracking
Common gaps: No MDM, personal devices accessing CJI, no remote wipe, unencrypted mobile storage
CoreReconOS coverage: Fortress — Mobile device management, encryption enforcement, remote wipe, GPS tracking

**John Martinez**
CEO & Founder, CoreReconOS
AT&T Vendor for State of Texas Incident Response | SDVOSB Certified
corerecon@polsia.app | corerecon.polsia.app