

CJIS Security Policy v6.1 and BrickStor SP

Criminal Justice Information ends up in files: case folders, digital evidence exports, and records attachments, stored beside body-worn video and interview recordings. BrickStor SP protects that data at the storage layer with FIPS 140-3 validated encryption, a per-file audit record, and Active Defense, on hardware that stays in your facility.

Your CJ I stays in your custody

BrickStor SP runs in your facility as a RackTop appliance, a gateway in front of storage arrays you already own, or a virtual machine. RackTop does not host or store your data and has no remote connectivity to your systems. When RackTop support helps your team, engineers work with system controls and configuration, never the contents of your files. Encryption keys stay with you in the built-in key manager or your own KMIP server.

What v6.1 means for storage

- CJIS now follows NIST SP 800-53 control families, each requirement with its own priority.
- SC-13 and SC-28 require FIPS 140-3 cryptography at 256-bit strength. FIPS 140-2 certificates are not acceptable after September 21, 2026.
- Existing and Priority 1 requirements, including MFA, are sanctionable now. Priority 2 to 4 requirements leave the zero cycle on September 30, 2027.

Control mapping for the storage that holds CJ I

Control	CJIS v6.1 asks	How BrickStor SP helps
Access Control and Identification & Authentication		
AC-2 NOW	Manage the account lifecycle and review accounts.	Local and AD or LDAP accounts with full lifecycle; disabled directory accounts lose access at next sign-in; every admin change is logged; rosters on demand for review.
AC-3, AC-6 NOW	Enforce approved authorizations and least privilege.	File and directory permissions enforced on every SMB and NFS access; ABAC labels from an external policy engine enforced; three management roles, including read-only.
AC-17 NOW	Authenticate and control remote access.	Hub console (TLS), SSH, REST API, and BMC all require authentication; per-dataset host restrictions.
IA-2 NOW	Uniquely identify users; MFA for privileged and non-privileged accounts.	Every file action tied to a unique identity; administrator sign-in supports passkeys (FIDO2) and one-time codes. File-share user MFA is enforced at directory sign-in.
IA-5 NOW	Manage authenticators and password policy.	Directory accounts inherit AD policy; local accounts support complexity, lifetime, and reuse rules, stored as SHA-512 hashes.
Audit and Accountability		
AU-2, AU-12 ZERO	Log defined events and generate audit records.	Hub audit log for every administrative action, User Behavior Auditing for file reads, writes, deletes, renames, and permission changes, plus the system log.
AU-3 NOW	Record what, when, where, source, outcome, and identity.	Event type, UTC timestamp, user and role, client IP, protocol, full file path, and outcome on every record.
AU-6 NOW	Review and analyze audit records weekly.	Hub audit views and user behavior reports; Active Defense analyzes file activity continuously and responds in real time.
AU-9 NOW	Protect audit information from unauthorized change or deletion.	Audit access limited to management roles, with a read-only reviewer role; all streams forward to your SIEM over TLS syslog (RFC 5424 or CEF), outside any storage admin's reach.
AU-11 NOW	Retain audit records at least one year.	Local retention by time and capacity, plus copies on a replication partner and in your SIEM.

Control	CJIS v6.1 asks	How BrickStor SP helps
System and Communications Protection		
SC-8 NOW	Protect CJI in transit.	TLS 1.2 or 1.3 and SSH v2 for management, TLS for replication, SMB3 encryption, NFSv4 with Kerberos (krb5p).
SC-12 NOW	Establish and manage cryptographic keys.	Per-dataset keys with rotation in the built-in key manager (replicated to a peer for backup) or your KMIP server.
SC-13, SC-28 NOW	FIPS 140-3 cryptography at 256-bit strength; encrypt CJI at rest outside physically secure locations.	AES-256 per-dataset encryption with a FIPS 140-3 Level 1 validated module (CMVP #5423) in BrickStor SP 23.9 and later, plus FIPS 140-3 Level 2 validated self-encrypting drives in RackTop appliances shipped since 2022 with FIPS drives.
Contingency Planning		
CP-9 ZERO	Back up user and system information; protect backups.	Policy-driven immutable snapshots; replication over TLS to a second BrickStor with keys forwarded; ImmutaVault isolated copies that survive administrative compromise.
CP-10 ZERO	Recover and reconstitute to a known state.	Highly available controllers, a read-only operating system, and Intelligent Bulk Remediation, which restores only the files an attack touched.
System and Information Integrity and Incident Response		
SI-3, SI-4 NOW	Detect malicious code and monitor the system.	Active Defense detects ransomware, mass deletion, data theft, and unusual access, opens an incident in real time, and can block the user or client.
SI-7 NOW	Verify software and information integrity.	Signed packages, boot-time verification, a read-only OS image, and self-healing checksums on stored data.
IR-4 NOW	Handle incidents.	Automated responses (block user, block client, hold snapshots, notify) and an incident record in the Hub console.
IR-6 ZERO	Report suspected incidents within one hour; automate reporting.	Incidents pushed automatically to Teams, Slack, PagerDuty, your SIEM, or email.

Now = tagged Existing or Priority 1 in CJIS v6.1, sanctionable since October 1, 2024. **Zero** = Priority 2 to 4 modernized requirement in the zero cycle through September 30, 2027. Source: FBI CJIS Security Policy v6.1 (June 25, 2026) and the RackTop NIST SP 800-53 Rev. 5 crosswalk for BrickStor SP.

What your agency still owns

- MFA for officers and staff at workstation and directory sign-in.
- Weekly audit review, and forwarding audit records to your SIEM.
- Local password policy, and changing factory and BMC default credentials.
- Turning on dataset encryption at creation and enrolling the self-encrypting drives. The drive layer applies to RackTop appliances, not SAN gateway or virtual deployments.
- Reporting incidents within one hour to your CSO and the FBI CJIS ISO.
- Confirming vendor agreements with your CJIS Systems Agency.

No product is "CJIS certified"

The FBI does not certify or endorse products against the CJIS Security Policy, and there is no national CJIS certification for technology. Compliance is assessed at the agency by its CJIS Systems Agency. Judge a storage platform on the controls it supports and the evidence it produces for the auditor.

Built for evidence at scale

Sheriff's offices and local municipalities run BrickStor SP for forensic evidence, body-worn camera footage, and fixed building-camera video today, several for more than five years. It scales from a single terabyte to multiple petabytes, and patented Transparent Data Movement moves aging video to lower-cost storage while each file keeps its original path.

Next step: ask RackTop for the full NIST SP 800-53 crosswalk and a walkthrough of this mapping against your environment, or see Active Defense stop a live attack: racktopsystems.com/solutions/law-enforcement