Justice Innovations Intake Platform

Security & Compliance White Paper

Executive Summary

The Intake Platform is engineered for prosecutors, law enforcement, clerks, and jail staff operating in CJIS- and FedRAMP-governed environments. The system safeguards Criminal Justice Information (CJI) through strict encryption standards, immutable audit logs, zero-trust principles, and a secure GovCloud architecture that exceeds state and federal requirements. This white paper outlines the platform’s technical, operational, and governance controls that ensure security, integrity, and confidentiality throughout the lifecycle of criminal case data.

1. Security Architecture Overview

1.1 Zero-Trust Design

- Every request authenticated and authorized.
- Role-based access with least-privilege policies.
- No implicit trust across internal services; all traffic authenticated.

1.2 GovCloud Infrastructure

- Hosted in AWS GovCloud (US), meeting FedRAMP Moderate baselines.
- All CJI processed and stored exclusively within GovCloud boundaries.
- Infrastructure access restricted to CJIS-screened personnel.

1.3 Network Security

- Enforced TLS 1.2+ (TLS 1.3 preferred).
- PrivateLink and VPC peering for agency integrations.
- No public endpoints for CJI data transfer.
- Optional SFTP/secure VPN channels for high-security ingest.

2. Data Protection Controls

2.1 Encryption Standards

- **At rest**: AES-256 (FIPS-validated).
- **In transit**: TLS 1.2+/1.3.
- **Key management**: AWS KMS (FIPS 140-2 validated).

2.2 Evidence Handling

- SHA-256+ hashing on ingestion.
- Re-hash verification at each access.
- Immutable chain-of-custody tracking.
  All media stored in encrypted secure buckets with access logging.

2.3 Sensitive Identifiers

- SSNs, DOBs, biometrics encrypted with field-level security.
- Masked views available for non-privileged roles.

3. Identity, Access, and Authentication

3.1 Multi-Factor Authentication

- MFA required for all users.
- Supports app-based authenticators and hardware tokens.

3.2 Role-Based Access Control

- Strict RBAC: Officer, Prosecutor, Clerk, Jail, Judge, Admin.
- Case-level and data-type-level permissioning.
- Automatic revocation upon separation or inactivity.

3.3 Identity Proofing

- NIST IAL2/AAL2 alignment for agencies that require verified identities.

4. Logging, Monitoring & Audit

4.1 Immutable Logs

- Write-once, tamper-evident log storage.
- All events logged: authentication, case actions, evidence access, filings.

4.2 Continuous Monitoring

- Automated anomaly detection.
- Real-time alerts for unauthorized access attempts.

4.3 Audit-Ready Reporting

- On-demand audit summaries for court requests, subpoenas, IA reviews.
- Quarterly log review by CJIS-screened administrators.

5. Compliance Alignment

5.1 CJIS Security Policy

- Authentication, encryption, network isolation, audit controls mapped to CJIS Sections 5.4–5.13.
- Media sanitization per CJIS 5.8 and NIST 800-88 Rev.1.
- Incident response following CJIS-aligned breach notification timelines.

5.2 FedRAMP Moderate

- Controls implemented across AU, AC, SC, IA, IR, MP, PE, PL families.
- SSP available for agencies upon request.

5.3 State & Local Requirements

- Retention policies respect jurisdictional statutes.
- Evidence preservation policies designed for appeal windows and post-conviction access.

6. Data Lifecycle Management

6.1 Retention & Purge Logic

- Case data: retained per state felony/misdemeanor rules.
- Evidence: retained through disposition + appeals.
  No deletion without dual authorization.

6.2 Sanitization & Archival

- Secure archival for long-term storage.
- Sanitization procedures follow NIST 800-88 Rev.1 for media disposal.

7. Incident Response & Continuity

7.1 Incident Response

- Dedicated IR plan for CJI-related events.
- Root-cause analysis and post-incident reporting included.

7.2 Business Continuity

- Daily encrypted backups.
- Multi-AZ redundancy.
- Disaster recovery testing.

8. Agency Onboarding & Governance

- Full CJIS onboarding packet available.
- Administrator training + certification.
- Documentation: SSP, SOPs, audit procedures, evidence integrity workflows.

Conclusion

The Intake Platform is built to exceed the security, compliance, and evidentiary integrity needs of modern criminal justice agencies. Its architecture ensures prosecutors, officers, and clerks operate within a trusted environment that maintains confidentiality, protects evidence, and withstands scrutiny in court and in audits.