WHITEPAPER

Mapping Zero Trust to CJIS Framework

A Modern Approach for Achieving Mandatory Compliance Standards

Overview

The following maps network and security requirements of the Criminal Justice Information Services (CJI) Security Policy to Nile's Network-as-a-Service architecture and shared-responsibility model.

- **Core Positioning:** Nile fully aligns to defined CJIS requirements.
- **Nile Contribution:** Secure-by-default access infrastructure, segmentation, posture enforcement, logging, monitoring, and patching.
- **What Customers Retain:** Identity, application access, CJI handling, compliance-specific policy decisions, and final authority signoff.

What is the CJIS Security Policy?

The FBI CJIS Security Policy governs how criminal justice agencies protect Criminal Justice Information (CJI). For networking teams, the operational burden is not just implementing controls but continuously maintaining and proving them during audits.

The policy spans personnel security, physical access, audit and accountability, system and communications protection, and access control. For agencies running traditional wired and wireless infrastructure, many of those requirements become a long checklist of per-device settings that must be configured, monitored, and revalidated over time.

Nile changes that operating model. Instead of asking the customer to keep each infrastructure element compliant through manual configuration, Nile delivers a deterministic network service in which segmentation, deny-by-default access, centralized telemetry, and patch currency are structural properties of the architecture.

This distinction matters in a triennial audit. Auditors do not only ask whether a control exists. They ask whether it is current, consistently applied, and demonstrable. A zero-trust, cloud-operated service makes that evidence easier to produce because the control state is centralized rather than scattered across devices.

Boundary Protection: Firewall and Network Segmentation

CJIS expects agencies to monitor and control communications at external and internal boundaries, separate critical traffic, and enforce deny-by-default behavior.

Requirement SC-7: Monitor and control communications at managed interfaces, separate subnetworks, and deny network communications by default while allowing only explicitly authorized traffic.

Nile's Zero Trust Fabric enforces segmentation as an architectural property, eliminating a legacy VLAN-by-VLAN configuration exercise. Every device is placed into an isolated segment by default, and traffic between devices, groups, and sensitive zones is blocked unless policy explicitly allows it.

This is especially relevant for CJIS environments where agencies need a privileged CJI access zone. Nile can create a dedicated CJI segment that only approved users and devices can reach, while micro-segmentation limits accidental or unnecessary adjacency elsewhere in the environment.

Why this matters in an audit

- No open-by-default network state to explain later.
- No dependence on individual AP or switch configurations to maintain isolation.
- Reduced risk that an expansion, replacement, or reset device reintroduces exposure.

Customer Responsibility

- Define which users, devices, and applications should be allowed into CJI-related segments.
- Create allow/deny flows that align with agency policy and operational needs.

Wireless Data Transmission and Authentication

CJIS Section 5.13.1.1 imposes detailed wireless requirements that traditionally become a per-device compliance burden.

Requirement 5.13.1.1: Validate rogue access points, secure management access, eliminate weak defaults, use strong encryption, disable unnecessary protocols, isolate wireless from operational wired infrastructure, and maintain logging.

Nile's managed wireless architecture collapses many of these discrete checklist items into centrally enforced service properties. Rogue AP detection is supported through WIDS/WIPS, access point inventory is continuously maintained, and compliant SSID, management, and encryption settings are applied uniformly across the deployment.

Because administrators do not manage local per-device interfaces in the traditional sense, Nile removes common sources of audit findings such as factory-default SSIDs, forgotten password rotation, exposed management protocols, or missed logging enablement on individual devices.

Requirement	Nile Responsibility	Customer Responsibility
Rogue AP detection and inventory	Continuous WIDS/WIPS monitoring and authoritative AP visibility to reduce the risk of unknown or unmanaged wireless devices.	Use of alerts and related procedures within the agency's broader incident handling program.
SSID and management security	Centralized, uniform configuration to prevent replacement or reset APs from drifting into non-compliant defaults.	Define naming and policy conventions that align with agency standards.
Wireless-to-wired isolation	Structural segmentation structural, which supports CJIS expectations for insulating wireless from operational wired infrastructure.	Approve the business flows that must cross those boundaries.

Cryptographic Protection: Wireless Data Transmission

CJIS distinguishes between wireless encryption requirements and the broader requirement for FIPS-validated cryptographic protection of CJI in transit.

Requirement SC-13: Protect CJI in transit with approved cryptographic mechanisms, while ensuring wireless infrastructure uses strong encryption and avoids deprecated protocols.

Nile supports strong wireless encryption, including WPA3-based implementations that meet the CJIS expectation for modern encryption strength on the access network. Nile also encrypts transport between network elements and the Nile cloud service plane.

In most CJIS deployments, however, the decisive encryption control for actual CJI sessions is implemented by the application or VPN layer rather than by the access network. That means customer-managed CJI applications, state connectivity methods, VPN clients, and related cryptographic modules remain central to end-to-end compliance.

Nile Contribution

- Strong wireless encryption on the access network.
- Encrypted transport between Nile network elements and Nile cloud services.
- No default shared keys or weak legacy-management patterns in the access fabric.

Customer Responsibility

- Ensure application-side or VPN-side protection for CJI sessions.
- Validate certification status and authority guidance for the cryptographic components that actually protect CJI content.
- Own encryption at rest in agency applications, databases, and systems of record.

Access Control: Identity-Based Enforcement and Lateral Movement Prevention

CJIS expects authenticated, authorized access tied to approved users and controlled remote or wireless access paths.

Requirements AC-2, AC-17, AC-18: Grant access based on authenticated identity, limit access according to role and purpose, and ensure wireless and remote access are controlled rather than trusted by network location alone.

Nile enforces access at the network layer based on authenticated user and device identity, not merely where a device plugs in or by IP/MAC address. Agencies gain a second enforcement layer in addition to application authorization that enables immediate, infrastructure-wide policy updates without changing individual configuration values on every device.

Per-device isolation further strengthens the posture by preventing malware, ransomware, or unauthorized devices from moving laterally just because they are connected to the network. Where required, Nile can also quarantine devices that do not meet a defined security posture before they can access a CJI segment.

Nile Contribution

- Deny-by-default access at the network layer.
- Per-user and per-device identity-based policy enforcement.
- Device posture checks before sensitive access.

Customer Responsibility

- Manage identity systems, MFA, application authorization, and user lifecycle processes.
- Define the posture standard and maintain endpoint security tooling.
- Own the final access-level model for CJI workflows and applications.

Audit and Accountability: Logging and Monitoring

CJIS requires audit records that establish what occurred, when it happened, and who was involved. Traditional infrastructure often makes that evidence hard to assemble.

Requirement AU: Capture and retain audit-relevant records for network authentication, access decisions, and management activity, and make them usable for monitoring, investigation, and compliance evidence.

Nile continuously aggregates authentication records, policy enforcement decisions, configuration activity, and network events through a centralized management plane. This removes a common compliance failure in traditional environments: the silent gap created when an individual device was never configured, or is no longer configured, to forward logs.

Nile also generates security events that can support threat detection workflows and downstream monitoring platforms. Agencies gain a cleaner path to investigations, retention, and evidence collection versus manually extracting records from distributed devices during an audit.

Nile Contribution

- Audit trail of network access and settings changes.
- Continuous audit logging of management and configuration activity.
- Security event generation for SIEM and broader monitoring workflows

Customer Responsibility

- Integrate logs into the agency monitoring stack.
- Apply retention, review, escalation, and investigation procedures.
- Correlate network-layer records with application and user-layer evidence.

Configuration Management: Vulnerability Management and Patching

Keeping infrastructure current is a recurring burden in conventional networks and a frequent source of compliance drift.

Requirements SC-10, Config Mgmt: Keep network infrastructure current through timely remediation and enforce session-management expectations without depending on inconsistent local administration.

Nile performs software updates, firmware remediation, and vulnerability management for Nile-owned infrastructure as part of the service. That materially reduces the operational overhead on agency IT teams and strengthens audit posture by making patch currency demonstrable from a centralized system. Verification of updates is performed against per-site AI-driven Nile Digital Twin technology.

For the customer, this means the access network no longer competes with mission systems for scarce maintenance time. It does not remove responsibility for patching endpoints, applications, identity systems, or other non-Nile components, but narrows the scope of what the agency must maintain directly.

Shared Responsibility Matrix

What Nile covers and what it does not

The most accurate customer-facing message is not that Nile "makes you CJIS compliant," but that Nile materially strengthens and simplifies the infrastructure portion of a CJIS-aligned deployment.

Control Area	Nile Contribution	Customer Responsibility	Ownership
Scope boundary and CJI handling	Provides wired & wireless access infrastructure and is typically not the system that stores, processes, or broker-transmits CJI.	Owns the applications, workflows, & systems that access, store, process, or transmit CJI.	Split by function
Access control & Authentication methods	Adds a second enforcement layer through network access policies & micro-segmentation. Delivers secure wired and wireless integration points with secure default port behavior.	Manage user & application authorization, along with compliance-specific policy design. Define SSID, port, identity, and authentication mechanisms.	Shared
Encryption in transit	Supports strong access-network encryption & encrypted transport in the Nile Zero Trust Fabric path.	Ensure end-to-end encryption for CJI sessions at the application or VPN layer.	Shared
Segmentation and privileged CJI zones	Supports native micro-segmentation and separate CJI access segments.	Define the segment design, approved groups, and business-approved flows.	Shared
Lateral movement prevention	Places devices into isolated segments by design and blocks traffic unless policy permits it.	Decide when limited flows between segments should be opened.	Shared
Device posture and quarantine	Can enforce threshold posture requirements before sensitive access is granted. Strengthens quarantine by eliminating traditional VLAN required device configuration changes.	Define posture standards and run the endpoint security program.	Shared
Audit logging and security events	Provides network access logs, settings-change trails, and security events.	Integrate, retain, investigate, and operationalize those logs.	Shared

Conclusion

The central argument for a modernized CJIS model is that compliance becomes more sustainable when the network's security properties are built-in rather than manually maintained device by device.

For law enforcement IT teams, the real challenge is rarely understanding what CJIS requires. It is maintaining those requirements consistently over time, staff turnover, hardware replacement, software updates, and audit cycles. Nile addresses this at the network layer by making segmentation, identity-aware access, telemetry, and patch currency properties of the service itself.

Nile supports CJIS-aligned deployments through secure wired and wireless access infrastructure, hardened service operations, segmentation, posture enforcement, logging, and patching within a shared-responsibility model.

That does not eliminate customer responsibility, nor should it be positioned that way. Identity, application access, CJI handling, physical controls, MFA, and agency-specific implementation decisions still matter. Nile does reduce the amount of compliance related manual tasks that depend on day-to-day device administration, which is where many organizations struggle most.

Disclaimer: *This document is an informational summary and does not constitute legal advice or a formal CJIS compliance determination. Final compliance depends on customer implementation and the applicable authority.*

About Nile

Nile is a pioneer and leader in secure networking-as-a-service (NaaS). With AI-powered service delivery and autonomous operations, Nile solutions cut through complexity and cost versus legacy networking solutions, while delivering radical operational simplicity and user experiences.