**Zero Trust Network Access (ZTNA) in Public Safety Environments**

**Introduction**

Public safety agencies face increasingly advanced cybersecurity threats as they manage sensitive criminal justice and emergency response data. Traditional perimeter-based security models that rely on implicit trust inside the network are no longer sufficient to protect against modern attacks.

Zero Trust Network Access (ZTNA) provides a comprehensive security framework that safeguards Criminal Justice Information (CJI), maintains operational continuity, and supports compliance with critical standards such as the CJIS Security Policy. This paper explores the principles of ZTNA, its relevance to public safety, and key considerations for building secure, future-ready environments.

---

**What is Zero Trust Network Access (ZTNA)?**

ZTNA is a security model that begins with the assumption that no user or device is inherently trusted, regardless of its location inside or outside the agency network. Access is continually evaluated and granted only based on verified identity, device posture, contextual signals, and clear policy enforcement.

**Key principles of ZTNA**

- **Verify explicitly**
  Authenticate and authorize every access request using strong identity controls and multiple independent factors.
- **Apply least privilege access**
  Limit data and system access strictly to what is necessary for each user role, reducing exposure of sensitive information.
- **Assume breach**
  Maintain continuous monitoring and visibility, operating under the premise that an attacker could already be inside the environment.
- **Implement micro-segmentation**
  Divide the network into isolated zones to prevent attackers from moving freely if one segment is compromised.
- **Build for adaptability and continuous improvement**
  Design architectures that can incorporate evolving security capabilities, such as

behavioral analytics and automated policy adjustments, as these become standard practice.

---

**Threat Model in Public Safety**

ZTNA directly addresses the primary threats faced by law enforcement and emergency services, including:

- External attackers seeking to steal credentials, deploy ransomware, or extract sensitive operational data.
- Insider threats or compromised legitimate accounts attempting unauthorized access to CJI.
- Advanced persistent threats (APTs) using stealth techniques to explore systems and exploit overlooked vulnerabilities.
- Lost or stolen field devices that may store session credentials or cached confidential data.

Implementing ZTNA mitigates these risks through strong identity verification, compartmentalized access, and continuous oversight.

---

**Why ZTNA for Public Safety?**

Public safety agencies manage mission-critical and highly confidential data, including criminal records, CAD and RMS incident data, and live emergency communications. ZTNA directly supports these environments by:

- Protecting CJI through explicit, context-driven authentication and authorization, defending against both internal misuse and external attacks.
- Enabling secure remote work and field operations without relying on broad, persistent VPN tunnels that increase the attack surface.
- Reducing the risk and potential impact of ransomware and targeted attacks by preventing unauthorized lateral movement within networks.
- Strengthening compliance with CJIS Security Policy, HIPAA, GDPR, and evolving state privacy regulations through structured identity management and comprehensive audit controls.

---

**ZTNA and CJIS Compliance**

The CJIS Security Policy requires rigorous authentication, role-based access control, data encryption, and thorough audit logging to protect CJI. ZTNA naturally aligns with these mandates by:

- **Enforcing Multi-Factor Authentication (MFA)**
  Ensures every access attempt is validated through multiple independent factors, regardless of location or device.
- **Implementing Role-Based Access Control (RBAC)**
  Restricts data and system permissions based on user job functions, enforcing least privilege as required by CJIS.
- **Securing data in transit with encryption**
  Applies TLS 1.2 or higher to protect communications and maintain confidentiality.
- **Maintaining continuous monitoring and audit logging**
  Provides real-time visibility and detailed records of access events for compliance reviews and investigations.

ZTNA deployments also typically include cryptographic key rotation and algorithm version tracking to maintain resilience as standards evolve.

---

**Evolving Toward Advanced Analytics and Machine Learning**

While current ZTNA implementations emphasize strong identity verification, least privilege enforcement, encryption, and continuous access control, the broader security industry is advancing toward integrating machine learning and advanced analytics into security operations.

Emerging solutions are expected to incorporate behavioral analytics that learn typical user and device patterns and identify deviations that could indicate compromised credentials or insider misuse. These capabilities require careful attention to data privacy, as logs used for detection often contain sensitive information that must be encrypted, access-controlled, and purged according to defined retention policies.

By adopting ZTNA now with architectures built on open standards and integration-ready APIs, agencies prepare themselves to incorporate these advanced analytics and automated response mechanisms when they become broadly operational and proven.

---

**Privacy and Data Minimization in Zero Trust**

A strong Zero Trust approach also embraces data minimization principles. Agencies should collect only the data necessary for operational mandates, limit how long data is stored, and apply anonymization or pseudonymization wherever practical. This practice supports compliance with GDPR Article 5, HIPAA Privacy Rule standards, and broader obligations to safeguard sensitive criminal justice and health-related data.

---

**Deployment Considerations and Best Practices**

When planning a ZTNA deployment in a public safety environment:

- Select solutions that are cloud-native or hybrid capable to support large, distributed workforces without introducing latency that could disrupt critical dispatch or investigation systems.
- Implement federated identity and open protocols such as OAuth2, OpenID Connect, and SCIM to support secure multi-agency collaboration and avoid vendor lock-in.
- Choose platforms that offer standardized APIs and log formats such as JSON, CEF, or LEEF, ensuring compatibility with existing security operations centers and future AI-driven systems.

---

**Case Study: ZTNA Preventing a Ransomware Breach**

A midsize police department experienced a ransomware incident after an officer's VPN credentials were compromised through phishing. Attackers used these credentials to move laterally, encrypt CAD systems, and exfiltrate sensitive case files.

By transitioning to a ZTNA architecture, the agency:

- Eliminated broad network tunnels, significantly reducing the attack surface.
- Enforced MFA and granular RBAC tied to specific officer and administrative roles.
- Established a foundation to adopt future AI-based monitoring by choosing open standards and implementing well-governed logging.

Following these changes, the agency improved its ability to detect and contain threats early, avoided further lateral breaches, and passed subsequent CJIS audits without deficiencies.

---

**Future-Proofing Against Cryptographic Risks**

Although current 2048-bit RSA encryption remains secure under all publicly known attacks, agencies should monitor advances in quantum computing and classical factoring algorithms. Preparing for post-quantum cryptographic standards, using elliptic-curve or hybrid schemes, and maintaining flexibility in cryptographic policies will help sustain long-term security as the technology landscape evolves.

---

**Why Public Safety Agencies Should Adopt ZTNA**

ZTNA rigorously controls access to critical systems and data through explicit identity verification and context-based decisions. It strengthens compliance with CJIS, HIPAA, GDPR, and state-level data privacy laws by enforcing multi-factor authentication, encryption, comprehensive audit logging, and least privilege principles. By removing implicit network trust and planning for future integration of advanced detection technologies, ZTNA reduces cyber risk while maintaining the operational flexibility essential to public safety missions.

---

**Glossary**

- **ZTNA:** Zero Trust Network Access, a security architecture that does not assume trust based on network location.
- **CJIS:** Criminal Justice Information Services Security Policy, which establishes federal standards for protecting law enforcement data.
- **RBAC:** Role-Based Access Control, restricting system access based on user job functions.
- **MFA:** Multi-Factor Authentication, requiring two or more forms of verification for access.

---

**References and Suggested Reading**


- NIST SP 800-207: Zero Trust Architecture (https://csrc.nist.gov/publications/detail/sp/800-207/final)
- FBI CJIS Security Policy (https://www.fbi.gov/services/cjis/cjis-security-policy)
- Gartner Market Guide for Zero Trust Network Access (https://www.gartner.com/document/3988994)

**Document published July 2025.** For technical inquiries, agencies should consult with their security leadership or technology partners experienced in public safety network security.

**About the Authors**

**Brian Nelson**
Brian Nelson is the founder and principal consultant at 911nurd, bringing more than 25 years of hands-on experience in public safety technology. His background includes decades managing, maintaining, and evolving critical 911 infrastructure, from CAD systems and telephony to radio networks and multi-agency operational platforms.

Brian partners directly with PSAPs, emergency management teams, and first responder leadership to modernize 911 environments, plan and execute complex system transitions, and ensure mission-critical resilience under demanding conditions. Known for his vendor-neutral perspective and practical problem-solving, he bridges technical design with the operational realities of public safety, helping agencies navigate next-generation network deployments, cybersecurity initiatives, and large-scale technology consolidations.

Earlier in his career, Brian served as a 911 Systems Administrator and project leader in Rock Island County, Illinois, where he oversaw system performance, compliance, and modernization for more than two decades. His experience is also grounded in military service as an aviation operations specialist and information systems analyst in the U.S. Army, adding a disciplined, mission-focused perspective to his work.

**Kenyon Langford**
Kenyon Langford is the Principal of 911nurd, where he leads strategic planning, financial stewardship, and operational oversight for technology initiatives serving the public safety sector. Drawing on more than two decades of executive leadership in IT, healthcare, and critical communications, Kenyon guides agencies through complex technology modernization projects and helps ensure secure, compliant deployments tailored to the unique demands of emergency services.

His experience spans roles as CIO and Vice President in healthcare and private sector technology environments, coupled with a deep focus on aligning business strategy with operational excellence. At 911nurd, Kenyon brings this background to the development and implementation of secure, next-generation public safety networks, fostering trusted partnerships and cultivating strong teams that support agencies' evolving needs.