WHITE PAPER

Cradlepoint Provides Connectivity for CJIS Security Policy Compliant Environments

Agencies can maintain CJIS compliance while leveraging the benefits of the cloud.

Overview

Cradlepoint has a long and successful track record of customers using Cradlepoint routers and NetCloud Service for securely transporting a wide range of sensitive federal, state, and local government workloads, including Criminal Justice Information (CJI) data. Law enforcement customers (and partners who manage CJI) utilize Cradlepoint Gigabit LTE enabled routers and NetCloud Service to easily extend and manage secure network connectivity to their policing vehicles, stations, and surveillance locations while maintaining CJIS compliance. The purpose of this paper is to provide information to law enforcement agencies on how to leverage and manage secure, Gigabit LTE router solutions that comply with CJIS Security Policy guidelines, while delivering significant ROI by reducing IT overhead costs, minimizing network downtime, and maximizing the effectiveness of law enforcement activities.

Cradlepoint provides wireless network edge solutions that include the use of advanced security protections such as intrusion detection and prevention, content filtering/anti-malware protection[1], IPSec VPN, private LTE networks, activity logging and alerting, FIPS 140-2 certified cryptographic modules[2], integrated permission management, and SD-WAN features to maximize uptime. By leveraging our FIPS-validated inside router models or integrating our non-FIPS routers with FIPS-certified software VPN clients, such as NetMotion, law enforcement agencies can maintain their CJIS security requirements while providing future proof Gigabit LTE connectivity to police stations, surveillance locations, and vehicles.

According to Cradlepoint statistics and research:

3,000

estimated number of **public safety agencies** that use Cradlepoint Service.

73%

of Police Departments **in the largest U.S. cities** use Cradlepoint Service.

4 OF THE 5

largest Police Departments have implemented Cradlepoint technology in the past 6 months.

What is the CJIS Security Policy?

The Criminal Justice Information System (CJIS) Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for the access to and safeguarding of CJI stored on FBI systems. The premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination, whether at rest or in transit, from unauthorized disclosure. This minimum standard of security requirements ensures continuity of information protection.

There are several roles defined within the CJIS Security Policy, all governed by the CJIS Advisory Policy Board (APB), which manages the policy with national oversight from the CJIS division of the FBI. These roles include the Terminal Account Controller (TAC) who "administers CJIS systems programs within the local agency" and the Local Agency Security Officer (LASO) who ensures "the approved and appropriate security measures are in place and working as expected," among other responsibilities[3]. The individuals holding these roles are most likely to coordinate with CJIS compliance auditors during mandatory triennial audits.

It is important to understand that there is no centralized adjudication body for determining what is or isn't compliant with the security policy in the way that FedRAMP has standardized security assessments across the federal government. In fact, the policy states that "not every consumer of FBI CJIS services will encounter all the policy areas, therefore the circumstances of applicability are based on individual agency/entity configurations and usage."[4] The individual agency/entity configurations and usage are specified in the Information Exchange Agreements executed between the FBI and each entity that is accessing CJI. Vendors/CSPs wanting to provide CJIS conformant solutions to multiple law enforcement agencies must integrate and/or conform to the applicable controls outlined in a CJA's Information Exchange Agreement, which are formal CJIS authorizations that vary from city, county, and/or state-level agencies.

Cradlepoint NetCloud Service is Designed with Security in Mind

Regardless of whether NetCloud falls within scope of an individual CJA's Information Exchange Agreement, Cradlepoint's Hardware-as-a-Service offering conforms to the requirements of the CJIS Security Policy. This includes utilizing FIPS compliant ciphers (Cradlepoint's Stream Protocol, which transports device management data between NetCloud and the device, utilizes TLS 1.2 with AES 256-bit encryption), the ability to force multi-factor authentication for all users within an account, and enforcing an organization's internal group/account security policies by configuring Federated ID/SSO. In addition to account and service security, NetCloud is hosted in physically secure AWS US regions with multiple AWS availability zones, hardware, storage, power redundancy, offsite backups, and has 99.999% availability.

[1] **Source** (Page 1) Additional license(s) required for IDS/IPS and Content Filtering

[2] **Source** FIPS Certified Cradlepoint router model required: IBR900F, IBR1700F or AER2200F

[3] **Source** CJIS Security Policy (08/16/2018) Section 3.2.3 and 3.2.9

[4] **Source** CJIS Security Policy (08/16/2018) Section 5, Par 3. (p. 14)

Cradlepoint delivers a secure and scalable NetCloud management service with high availability and dependability, providing the tools that enable customers to remotely administer and secure their mobile and branch routers from a single pane of glass. This secure service only maintains router configuration and management data and, thus, no customer network traffic, including CJI information, is sent to the cloud management service. Because Cradlepoint designed its cloud implementation with security in mind, Cradlepoint conforms to a wide range of regulatory requirements, including conformance with the CJIS Security Policy.

Cloud Applications, CJI & NetCloud Service

One of the topics for concern at state, county, and city law enforcement agencies is whether they can use cloud-based solutions for different use cases and to what degree.

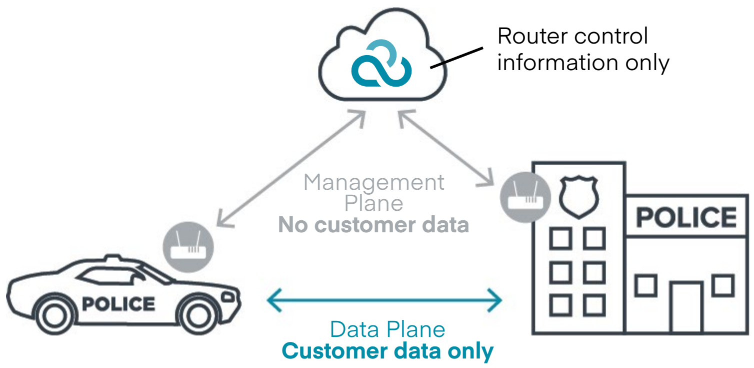
Unlike many of the compliance frameworks that AWS supports[6], there is no central CJIS authorization body, no accredited pool of independent assessors, nor a standardized assessment approach to determining whether a particular solution is considered "CJIS compliant." Simply put, a standardized "CJIS compliant" solution, which works across all law enforcement agencies, does not exist. It is often falsely misunderstood and miscommunicated that a cloud service provider can be "CJIS certified". It is necessary to understand that delivering a CJIS compliant solution using cloud services relies on a shared responsibility model between the cloud service provider and the CJA.

Many law enforcement agencies have questioned whether they can be compliant with CJIS Security Policy while using the cloud. The answer to this question is yes because the CJIS Security Policy is device and architecture

Many law enforcement agencies have questioned whether they can be compliant with CJIS Security Policy while using the cloud. The answer to this question is yes because the CJIS Security Policy is device and architecture independent.[5]

Cradlepoint's NetCloud Service is only concerned with securely transporting and storing router management data; no customer network data, to include CJI, encrypted or otherwise, is sent to NetCloud.

NetCloud Service Diagram Portraying Device Management Traffic Only to the Cloud



[5] **Source** CJIS Security Policy (08/16/2018) Appendix G.3 (pg. G-16)

independent.[5] In fact, cloud computing is specified within policy section 5.10.1.5 providing guidance and resources for enabling "organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy."[7] There are security challenges to overcome if using the cloud for transporting, accessing, or storing CJI data. However, NetCloud is only concerned with securely transporting and storing router management data; **no customer network data, to include CJI, encrypted or otherwise, is sent to NetCloud.**

2700+

public safety agencies
trust Cradlepoint.

CJIS Conformancy Within Law Enforcement Vehicles

Cradlepoint's products and services are purpose-built for distributed network use cases securely connecting branch, mobile vehicles, or IoT applications, especially for organizations with lean IT resources. Most law enforcement agencies have strong needs for a solution that can manage all of these use cases in a single service. The remainder of this paper will be focused on secure connectivity within law enforcement vehicles, which in of themselves can often be considered a mobile brick and mortar police station location. Section 5.9.1 of the CJIS Security Policy addresses physically secure locations, to include "a criminal justice conveyance," which is defined in the terms and definitions as "any enclosed mobile vehicle used for the purposes of criminal justice activities."[8] Within their vehicles, law enforcement personnel conduct the majority of their work on a Mobile Data Terminal/Computer (MDT/MDC). These MDTs host a variety of applications, such as Computer Aided Dispatch (CAD), Automatic Vehicle Location (AVL), and the application that has access to Criminal Justice Information (CJI). It is with the CJI application — how it connects and transports data to and from the FBI's CJIS databases, and the security mechanisms employed end-to-end — that the CJIS Security Policy is chiefly concerned with.

Cradlepoint Reference Architectures for Integration into CJIS Environments

Section 5.10: Information Flow Enforcement, of the CJIS Security Policy, specifically section 5.10.1.2.1: Encryption for CJI in Transit, explicitly specifies the requirement that "when CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption," and that "the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128-bit strength to protect CJI." Based on the encryption requirements and the fact that the vehicle is considered a physically secure location, Cradlepoint has identified two reference architectures that would comply with CJIS guidelines.

[5] **Source** CJIS Security Policy (08/16/2018) Appendix G.3 (pg. G-16)

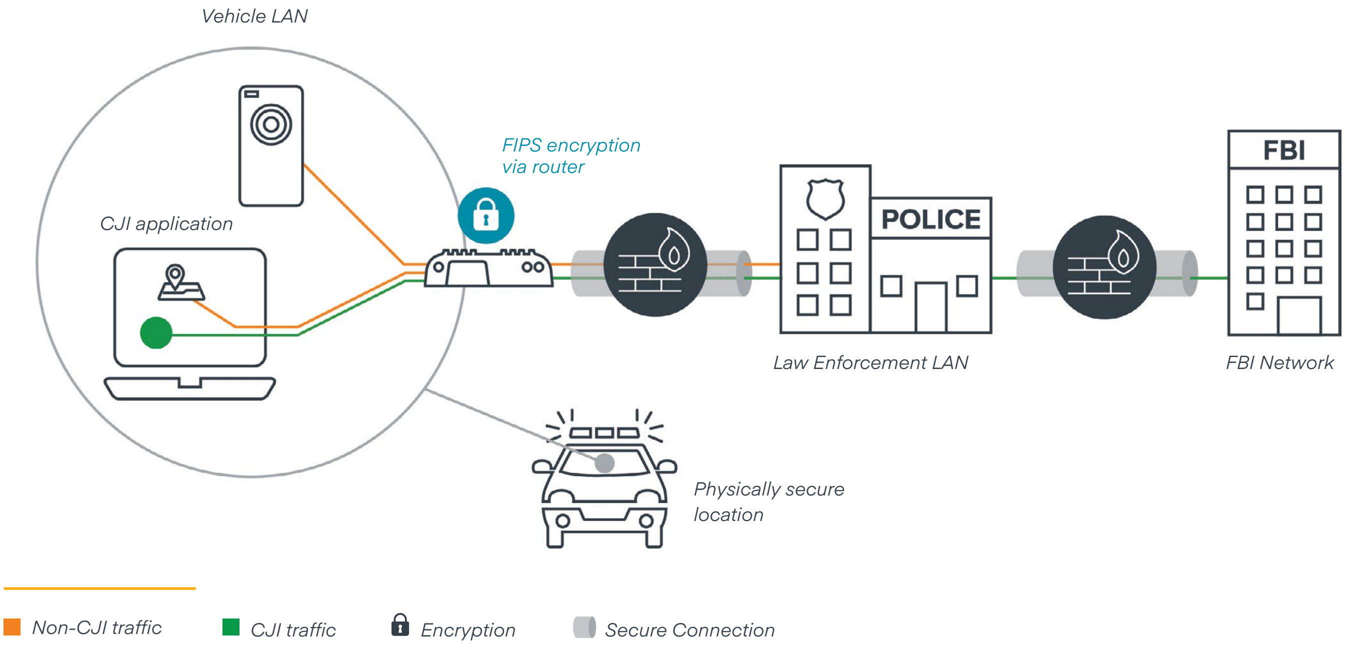
[6] **Source** https://aws.amazon.com/compliance/services-in-scope/

[7] **Source** CJIS Security Policy (08/16/2018) Section 5.10.1.5

[8] **Source** CJIS Security Policy (08/16/2018), Appendix A, Page A-4, Par. 4

FIPS Certified Router

This cost-effective approach leverages our Cradlepoint routers that include a FIPS-validated cryptographic module[9] built into NetCloud Operating System (NCOS). Cradlepoint FIPS routers are compatible with most VPN head end routers/firewalls and support most major routing protocols. By configuring VPN connections between the law enforcement internal network and the Cradlepoint router, a true site-to-site or spoke-to-hub VPN network connection can be established. This is useful if you host internal applications that remote devices, besides the MDT, require access to within the agency's internal network. It also mitigates the need for expensive software/client-based VPN solutions.



It's important to note that this reference architecture places the router and vehicle connectivity under additional scrutiny within the CJIS Security Policy and will require additional configuration and, possibly, additional advanced licenses to meet CJIS requirements, based on each individual CJA's Information Exchange Agreement. These additional configurations are tied to security features already present in all Cradlepoint routers, to include:

- Stateful zone-based firewall
- Intrusion detection/prevention system[10]
- Secure web filtering & anti-malware protection[11]
- RADIUS/TACACS+ support for device administration & WPA2 Enterprise WiFi network access[12]
- VLAN segmentation with admin access restrictions, MAC filtering & wired 802.1x support
- X.509 certificate & PKI infrastructure support
- Device logging & alerting with syslog support
- Automated enterprise-wide configuration management & security patching

[9] **Source** Nokia Cryptographic Module FIPS 140-2 Security Policy: https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2024.pdf (p. 3)

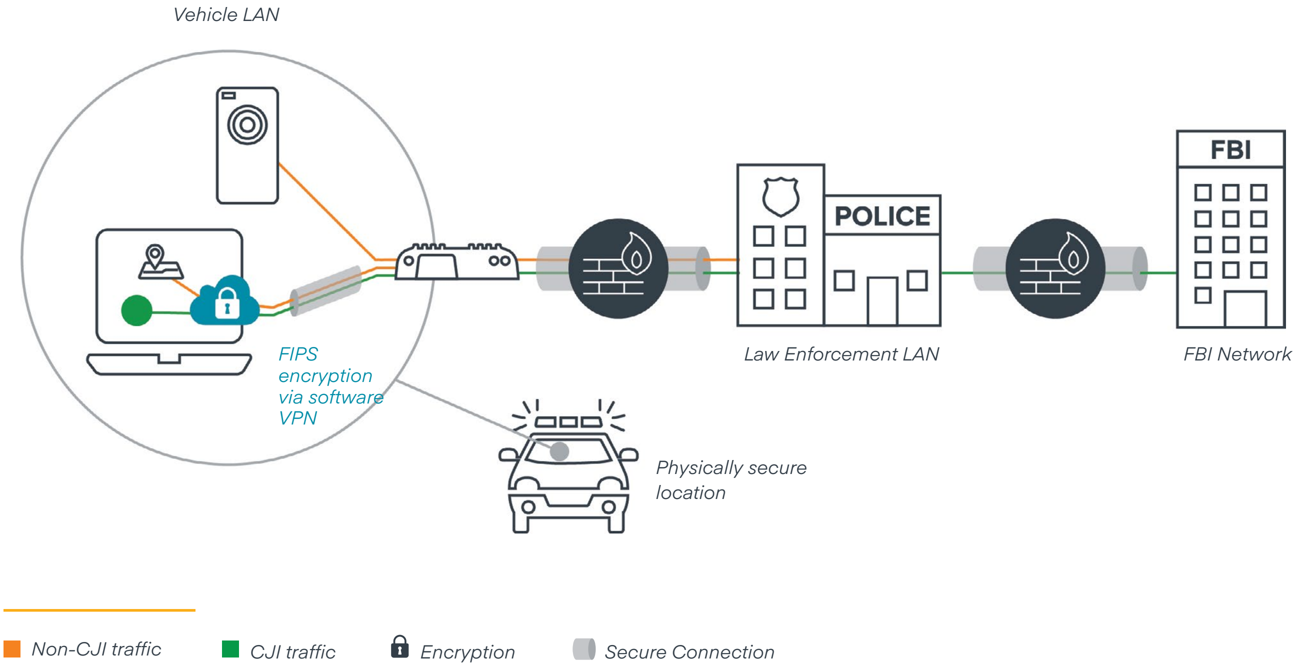
[10] **Source** IDS/IPS Engine powered by Trend Micro; additional license required

[11] **Source** CP Secure Web Filter powered by Webroot; Zscaler or Umbrella integration; additional license required

[12] **Source** See CJIS SP Section 5.13.1.1 for 802.11 Wireless Protocol requirements

Software/Client-based VPN

Most law enforcement agencies that use Cradlepoint devices also deploy VPN clients on their MDTs. This is because most MDT manufacturers, such as Panasonic, Getac, etc., include FIPS certified modules within their products. This is a great, albeit more expensive, solution as it restricts the requirements of the CJIS Security Policy solely to the MDT, mitigating the need for a FIPS-validated router and minimizing exposure of the agency's internal network to only the MDT itself. It also allows the law enforcement agency to take advantage of the additional features of the client VPN, such as application persistence with NetMotion.



Conclusion

At the end of the shift, law enforcement agencies, and the IT departments that support them, need to feel confident and assured that the architecture, solutions, and vendors they've chosen to deploy allow them to continue to meet their CJIS Security Policy requirements.

Deploying Cradlepoint not only helps build this confidence, it also provides the additional benefit of greater visibility, increased control, and more resilient connectivity, all while using less IT resources and delivering a significant return on investment.

Please note that the reference architectures presented in this paper are based on insights gained from the CJIS Security Policy revised August 16, 2018, and input from industry experts and law enforcement professionals. Before deciding on an architecture be sure to consult with your TAC and/or LASO and review your Information Exchange Agreement to ensure CJIS compliance. As you consider deploying Cradlepoint, expanding/refreshing your existing Cradlepoint devices, or adjusting your distributed network architecture, our experts stand ready to collaborate with you and your security team to ensure that you have the right solution for your agency.

About Cradlepoint

Cradlepoint is the global leader in cloud-delivered wireless edge solutions for branch, mobile, and IoT networks. The Cradlepoint Elastic Edge™ vision — powered by NetCloud services — provides a blueprint for agile, pervasive, and software-driven wireless WANs that leverage LTE and 5G services to connect people, places, and things everywhere with resiliency, security, and control.

More than 18,000 enterprise and government organizations around the world, including 75 percent of the world's top retailers, 50 percent of the Fortune 100, and first responders in 10 of the largest U.S. cities, rely on Cradlepoint to keep critical branches, points of commerce, field forces, vehicles, and IoT devices always connected and protected. Major service providers use Cradlepoint wireless solutions as the foundation for innovative managed network services. Founded in 2006, Cradlepoint is a privately held company headquartered in Boise, Idaho, with a development center in Silicon Valley and international offices in the UK and Australia.

Learn more at cradlepoint.com/law-enforcement-connectivity