thalestct.com

THALES

CJIS Data-in-Transit Encryption Standards

How to Address Your Criminal Justice Information Services Security Policy Requirements Effectively

White Paper

Contents

For US law enforcement agencies, complying with the Criminal Justice Information Services Security Policy (CJIS-SP) is an imperative requirement. However, it's also critical to ensure that the security mechanisms employed don't in any way impede staff in fulfilling the agencies' chief charter: fighting crime. This paper examines data-in-transit encryption, which is an important component of CJIS-SP requirements. It offers a number of insights into the approaches that can help organizations address data-in-transit encryption policies most efficiently and effectively—while ensuring that investigators and other users always get reliable, timely access to the information they need to do their jobs.

Reliance on Data Transmission—and Its Risks

As in virtually every industry, the digitization of information and ubiquity of high-speed connectivity have ushered in a fundamental transformation in the way law enforcement departments and agencies operate. To effectively pursue their law enforcement and administrative objectives, staff members now rely constantly on the fast transmission of information, including data being sent to and from CJI repositories. Consequently, large amounts of data are now routinely transmitted between offices and agencies, due to the evolution of data transmission speeds and pipeline throughput.

While this timely information sharing has yielded huge benefits in investigating crime, establishing evidence, and so on, it has also created risks. The broad transmission of massive volumes of sensitive CJI records also has increased the danger of this information falling into the wrong hands. Given the highly sensitive nature of CJIS data, these transmissions are increasingly being targeted by advanced cyber criminals and nation states.

Cyber-attacks continue to grow more sophisticated, and effective at evading organizations' security defenses, leading to a proliferation of breaches. Attacks have been attempted against a number of government agencies and police departments, such as the US State Department, US Investigations Services, California DMV, the Anoka County Sheriff's Office, and the Memphis Police Department. Outside of the US, a number of breaches have also been reported, including at the Australian Federal Police Department, where the metadata associated with phone calls made by a journalist were "illegally" accessed[1], Thames Valley Police in England[2], and others.

CJIS Security Policy

Given the sensitive, highly critical nature of the information that is exchanged within and among law enforcement agencies, standards have been developed in order to ensure rigorous safeguards are put in place. The CJIS-SP was instituted in an effort to provide an extensive set of guidelines and requirements surrounding the security of the source, transmission, storage, and generation of CJI.

The CJIS-SP applies to any organization that has access to CJI at any point in its lifecycle, from creation through dissemination. Organizations responsible for compliance are subject to audits by the FBI CJIS division at least once every three years.

The ultimate focus of the standard is to "provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit[3]." When it comes to data in transit, the standard states: "When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption)."[4]

It is important to underscore that this encryption requirement applies any time CJI is transmitted outside

a secure facility—even if the transmission is occurring between two offices within the same agency. Many security teams that have undergone CJIS-SP audits recently can attest to the fact that auditors are requiring the encryption of transmissions between an agency's distributed offices, just as they require encryption of the transmissions sent between different agencies.

The CJIS-SP offers both strategic and tactical guidelines enabling regulated agencies to select the security mechanisms that are aligned with their specific requirements.

While the guidelines lay out a set of standards and requirements, it is also important to stress that, while compliance is mandatory, it shouldn't be viewed as the primary objective—strengthening the security of CJI should be. Toward that end, security teams should look to employ technologies and approaches that strengthen the organization's controls around information access, sharing, and storage, enabling the organization to determine the most effective security policy, and to invest in the best security solutions available so they can establish maximum security against the evolving threats that confront agencies today. Further, as outlined in more detail below, it is also vital that any security mechanisms employed don't impede or slow staff members' ability to get the information they need to do their jobs effectively.

The following sections offer security teams an overview of some of the different alternatives they can use to address CJIS regulations for data-in-transit encryption, and it outlines some key characteristics to look for in evaluating encryption technologies.

Overview of Data-in-Transit Encryption Approaches

Most of today's networks are IP-based. This provides IT security teams with a decision point to decide how they encrypt data in transit and at what layer of the OSI model. In most scenarios, the choices are:

- Layer 2 Ethernet based encryption versus Layer 3 IPSec
- Stand-alone appliance versus integrated solution

Layer 2 Ethernet Encryption offers several distinct advantages over Layer 3 IPSec. Ethernet Encryption provides better bandwidth utilization along with lower and consistent latency. With Layer 2 Ethernet Encryption, line rate performance can be achieved, maximizing bandwidth utilization, preserving the investment made in the network, and optimizing ongoing operations. On the other hand, after implementing encryption at Layer 3, some organizations have seen the bandwidth available reduced to as little as 27% of prior levels. This bandwidth penalty only increases as the network scales to more connections and increased bandwidth per connection. At the same time Layer 2 solutions provided latency performance in microseconds while Layer 3 often results in latency in the milliseconds—a 10x performance hit. Further, Layer 2 solutions provide consistent latency performance for all packet sizes while Layer 3 solutions often have variable latency depending on packet size, causing what is known as "jitter", which can wreak havoc on real time applications. Layer 3 encryption approaches can have a negative impact on network scalability, operational effort, and cost.

Regarding stand-alone and integrated solutions, security considerations and performance need to be evaluated. Stand-alone appliances are dedicated "bump-in-the-wire" security devices built from the ground up to support all network equipment vendors and use cases. Integrated solutions are all-in-one networking or switching devices with integrated security and a host of other services running on a single platform. It is recommended that security and network architectures be separated to maximize security and performance. Encryption and network routing represent two very different functions, and running one platform that does two dissimilar things can mean that neither is done very well. From a security standpoint, integrated solutions often allow numerous users virtual and physical access. This increases the probability that the data or keys may be compromised. It also affects performance, since as the processing requirement increases, the encryption solution can become sluggish forming a bottleneck. Another concern is "vendor lock-in" as in-line security solutions are not compatible with other vendors' solutions. Therefore all future networking and security equipment will be tied to a single vendor or a "fork-lift upgrade" will be required to replace. Consequently, decoupling security from switching, and leveraging Layer 2 Ethernet platforms, is a best practice for most agencies. This approach enables IT organizations to select optimal solutions for their specific objectives and environments, so they can realize improved security, performance, and agility.

Interacting with Cloud Service Providers while Securing Data-in-Transit

More organizations are relying on the external expertise of cloud Service Providers to manage their cloud network requirements. It is important to remember that although a cloud Service Provider may be providing the network pipeline used to access the off-premise data, it is the sole responsibility of the organization to ensure that the cloud Service Provider is capable of meeting their security and encryption needs in order to stay CJIS compliant. When working with a cloud Service Provider, it is important to get clear and satisfactory answers to the following questions:

Encryption (section 5.10.1.2 of the CJIS-SP)

- Who will be providing the encryption as required in the CJIS Security Policy (the client or cloud service provider)?
- Is the data encrypted while at rest and in transit?

Audits by the FBI CJIS Division and the CSA (sections 5.11.1 and 5.11.2 of the CJIS-SP)

- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits?

Auditing and Accountability (section 5.4 Area 4 of the CJIS-SP)

- Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request?

Media Protection (section 5.8 Policy Area 8 of the CJIS-SP)

- What are the cloud service provider's responsibilities with regard to media protection and destruction?

What to Look for in a Layer 2 Encryption Solution

Security and Risk Mitigation

As mentioned earlier, rather than focusing on compliance, strengthening the security of CJI and other sensitive information should be the primary objective of any security initiative, and this holds true for data-in-transit encryption as well. Strong encryption offers a vital added layer of defense. For example, even if a network connection is hacked, the actual data being transmitted won't be decipherable or usable by the attacker.

In order to ensure that your organization passes its upcoming CJIS audits, and, most importantly, employs the highest level of security around sensitive data-in-transit, look to leverage encryption alternatives that deliver the following capabilities:

- **Certified high–assurance hardware appliances.** The CJIS-SP states that "When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards[5]." Look for appliances that offer FIPS 140-2 Level 3 as well as certification with other standards, such as Common Criteria. These standards certifications help provide assurances that the device has been vetted by independent agencies and rigorously tested to ensure:
  - the device is tamper-proof and will zeroize if opened, ensuring that there is no unauthorized access to the device
  - it supports the strongest algorithms such as RSA or ECC
  - it has a hardware-based, verified random number generator
- **Robust cryptography.** When employing encryption, the CJIS-SP requires a minimum of 128-bit cryptography. Look for solutions that offer support for AES 256-bit key sizes which can help provide high levels of security.
- **Strong key management.** Look for platforms that provide uncompromising protection of cryptographic keys. These keys should be kept in a certified (tamper-proof) hardware appliance at all times. In addition, look for platforms that offer hardware-based random number generation capabilities for key generation with a true random entropy source (FIPS certified).
- **Metadata protections.** The CJIS-SP standard expressly stresses the need to protect this information from the cloud provider, indicating "The metadata derived from CJI shall not be used by any cloud service provider for any purposes[6]." The metadata associated with network traffic can ultimately provide intelligence that can expose your organization. Look for offerings that can protect network metadata by combining traffic flow security (TFS) with Layer 2 Ethernet encryption, making traffic patterns and characteristics impervious to exposure through nefarious traffic analysis. This is especially critical for organizations that choose to work with cloud providers. Moreover, this will protect your metadata from being exposed by third parties or anyone else who is trying to hack your data and metadata

High Performance and Availability

For the users in your organization, gaining timely, dependable access to CJI is critical. Delays can compromise a range of urgent efforts, including emergency response, urgent investigations, and so on. Encryption shouldn't introduce poor performance or reduce reliability. That's why it's vital to leverage encryption platforms that provide maximum performance and availability, so you reduce the likelihood of outages or performance issues that affect users. To achieve these ends, look for platforms that offer:

- **High throughput.** Appliances should provide the performance required to secure time sensitive communications and applications. Look for appliances that are capable of running in full duplex mode, at full line speed, without introducing packet loss and near zero overhead
- **Minimal latency and jitter.** Platforms should introduce minimal latency. In addition, it is important that any latency that is introduced is highly predictable and not affected by packet size. Also, ensure that the platforms employed minimize jitter, which can degrade the user experience, particularly for voice over IP (VoIP) and video applications.
- **Predictability.** Look for appliances that have hardware-based "cut through" architecture enabling capabilities such as standard, field-programmable gate array (FPGA) capabilities, which help enable predictable and dependable performance as compared to solutions that utilize store and forward (buffering).

In addition, reliability isn't just important for end users. It's also important for the IT team. Toward that end, look for platforms that have been proven to run for years without incident, including in performance-intensive environments. Platforms should provide at least 99.95% uptime. Also look for adherence to industry safety and environmental standards.

Optimal Flexibility

The encryption requirements of your agency will often vary substantially from those of another. Further, the requirements and priorities your platform needs to address may change over time. It is therefore important to look for pragmatic solutions; ones that provide maximum flexibility in adapting to your specific infrastructure, threats, and objectives, both now and over time.

Following are a few capabilities that help foster flexible implementation:

- **Extensive network support.** Look for solutions that are compatible with leading network protocols such as Ethernet, STP (Spanning Tree Protocol), and Shortest Path Bridging (SPB). Look for platforms that enable flexible, efficient implementation in a range of Ethernet networks, including Layer 2 VPNs such as MEF services and VPLS. These solutions should also offer support for deployment in Ethernet networks with various architectures, including multi-point to multi-point (mesh), single-point to multi- point, and single point-to-point environments. Finally, they should also support unicast, broadcast, and multi-cast environments. The solution should be optimized for LAN/MAN/WAN environments, enabling full path encryption rather than hop-to-hop encryption.
- **Scalable throughput.** Look for platforms that can meet your organization's throughput demands, both initially and in the long term. Toward that end, it will often be advantageous to leverage platforms that can support low—end requirements today, such as 10 Mbps, while enabling you to scale to 10 Gbps, or even 100 Gbps over time.
- **Broad environment support.** Solutions that offer attributes like non-disruptive deployment and in-field upgradeability can be efficiently deployed and run in a range of computing environments.
- **Flexible deployment and solution options.** Any Layer 2 encryption alternative you select should offer support for deployments in single locations, and in complex environments that span multiple locations. Also, the vendor you work with should offer several deployment options, according to your specific needs and objectives. Look for vendors that offer families of products that run on the same protocols, that are fully interoperable, and that offer backward compatibility, so they can easily be adapted to changing requirements.
- **Administrative flexibility.** To provide optimal administrative efficiency, endeavor to adopt Layer 2 encryption platforms that can be managed locally, as well as through management software that can be used to control many distributed appliances. For many organizations, it is also advantageous to leverage management software that can function as a certificate authority for X.509 certificates.
- **Administrative ease and efficiency.** If you will be opting to manage multiple appliances centrally, look for platforms that enable you to leverage intuitive, Web- based interfaces. The process of deploying management capabilities should be done in minutes. Once deployed, administrators should be able to set appliances and forget them.

Low Cost and Ease of Use

As critical as the implementation of data-in-transit encryption is, like any other investment, selecting this type of solution has to be made in accordance with budgetary constraints and staffing realities. It is important to select solutions that address security and availability requirements, while minimizing cost and administrative overhead. Toward that end look for these features:

- **Unobtrusive implementation.** Layer 2 encryptors should offer a deployment design that enables you to install them in the network, without having to change the network architecture or any associated devices. The solution should also feature link-state forwarding that supports transparent implementation.
- **Maximum network flexibility.** It's important to choose a solution that enables the flexible implementation of security policies, and can be easily installed into any new network. Ensure that the solution is vendor-agnostic so it does not limit future connectivity in mixed environments when faced with different network protocols and other variables.
- **Rate limiting.** IT and security teams should look for offerings that can scale in throughput. In addition, try to find platforms that can be rate limited, which means you can buy an appliance with 10 Gbps of throughput, but only use 2.5 Gbps initially, and then increase capacity as your needs change.
- **Resource efficiency.** Look for platforms that have minimal footprints in the data center, both in terms of rack space and power utilization. (Size, Weight and Power - SWaP).

Risks of Non-CJIS Compliance

When you are not in compliance, you are always at risk.

In this scenario, there are several risks that should be considered if the decision to ignore CJIS compliance is made. The FBI provides a Security Addendum[7] with the CJIS Security Policy, and its purpose is to certify the understanding of the signer with regard to what is considered the minimum description of data misuse, and the corresponding degrees of penalty, which include, but is not limited to:

- **Loss of access to CJIS database.** If an audit is conducted and an organization is found to be non-compliant to the CJIS Security Policy, their access to the CJIS database and community can be revoked, and the organization will no longer be able to access the critical data that is necessary to perform essential duties, effectively cutting the organization from mission-critical information on-demand. In order to protect the security and integrity of the CJIS database and its member community, the FBI will consider revoking the access of those who choose non-compliance.
- **Loss of employment.** If an audit is conducted and an organization is found to be non-compliant to the CJIS Security Policy and the decision maker decides to continue operations without acquiring compliance, it can result in loss of employment if the organization's data is breached – especially if the root cause of the breach is proven to stem from non-CJIS compliance. At that point, the fault would lie with the decision maker, and bringing unwanted negative press to an organization, along with the added costs of resolving the breach, are usually enough to force the organization's hand to terminate the employment of the decision maker.
- **Prosecution at the State or Federal level.** The FBI may consider bringing legal action against non-compliant organizations who misuse CJIS data. The laws concerning data misuse differ at the state and federal levels, so multiple infractions may be placed upon an organization depending on the state the infractions take place in.

Conclusion

Addressing CJIS-SP requirements for data-in-transit encryption represents a baseline requirement for many law enforcement agencies today. However, security teams should focus their efforts on more than compliance and take the steps necessary to maximize the security of the sensitive data they work with. While the standard offers a lot of clear guidance, the reality is that IT organizations should select the best solution to secure their data and meet CJIS-SP requirements. By leveraging the right Layer 2 encryption platform, agencies can ensure not only that they'll pass their upcoming CJIS audits and optimize their high-speed network utilization, but most importantly, they'll strengthen their ability to guard against prevalent threats.

Thales Encryption Solutions

If your data is worth anything, it's worth encrypting. Thales is a global leader in the development of end-to-end encryption technologies. Our solutions protect sensitive data for a wide range of commercial, government, industrial and defence customers. From certified high-assurance hardware and virtualised encryption to secure file-sharing; all Thales solutions share a common high-performance encryption platform and are used to protect sensitive network data around the world.

Thales encryption solutions have been trusted to protect much of the world's most sensitive information for more than 20 years. They are used to protect everything from government and defense secrets to citizens' identity and intellectual property, financial transactions to real-time CCTV networks and critical national infrastructure control systems. Thales encryption solutions are available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies.

Hardware Encryption

Thales Network Encryptors deliver high-assurance encryption for core network and IT infrastructure. Certified by leading independent authorities (Common Criteria, FIPS and NATO), Thales CN Series encryptors provide maximum security and data protection for public and private networks. Operating from ultra-fast 100 Gbps to modest 10 Mbps bandwidths, they feature near-zero latency and overhead. Purpose built, secure and dedicated network encryption appliances; Thales CN encryptors provide maximum data protection and network security, without compromising network or application performance.

Virtual Encryption

The Thales CV1000 Virtual Encryptor (CV1000) delivers strong and flexible encryption security for virtual customer premise equipment (VCPE) and wide area networks. Scalable to thousands of endpoints, the CV1000 is a software application of the trusted Thales encryption platform. It delivers cost-effective, multi-layer data protection at up to 5 Gbps (with DPDK) bandwidth for cloud, distributed and software-defined networks. As a Virtual Network Function, the CV1000 is designed to meet the security and agility demands of virtualized data networks. It enables rapid encryption deployment to the virtual network edge.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com

[4] U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, "Criminal Justice Information Services (CJIS) Security Policy", Version 5.6, page 64

[1] Huffington Post, "Federal Police 'Illegally' Accessed a Journalist's Metadata", April 20, 2017, http://www.huffingtonpost.com.au
[5] U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, "Criminal Justice Information Services (CJIS) Security Policy", Version 5.6, page 64

[2] Daily Mail, "Corrupt policewoman who stole details of 2,500 road crash victims from force database for no-win no-fee scam jailed for three and a half years", March 12, 2014, http://www.dailymail.co.uk
[6] U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, "Criminal Justice Information Services (CJIS) Security Policy", Version 5.6, page 58

[3] U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, "Criminal Justice Information Services (CJIS) Security Policy", Version 5.6, page 217
[7] U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, "Criminal Justice Information Services (CJIS) Security Policy", Version 5.6, pages 206-212