CERTES NETWORKS

CERTESNETWORKS.COM

WHITE PAPER |

CJIS Security Policy - Data in Transit

Overcoming the Challenges of Encrypting Data in Transit under CJIS Security Policy Requirements

Today's law enforcement agencies and non-criminal justice agencies require access to essential Criminal Justice Information Services (CJIS). To keep this access complying with the FBI's CJIS Security Policy is mandatory.

One of the biggest challenges for agencies is meeting the requirement to encrypt data in transit.

This paper examines these requirements and makes suggestions for how to overcome them.

What is CJIS?

CJIS is a division of the FBI. This division operates several key law enforcement databases. Agencies (and non-criminal justice agencies) rely upon these databases for daily operations. Some of the information databases administered by CJIS are:

- **National Crime Information Center (NCIC)** which helps with many functions including locating missing persons and apprehending fugitives
- **National Data Exchange (N-DEx)** System which provides agencies with an online tool for sharing, searching, linking and analyzing information across jurisdictional boundaries
- **National Instant Criminal Background Check System (NICS)** and the **Next Generation Identification (NGI)** system which is a repository of biometric and criminal history information.

What is the purpose of the CJIS Security Policy?

Due to the sensitive nature of the data contained throughout the CJIS database services it is vital to protect that data from falling into the wrong hands.

The purpose of the CJIS Security Policy is to provide a minimum set of security requirements that must be adopted by any agency that accesses the CJIS division database services.

The security requirements ensure that the handling, storage and transmission of CJI is protected appropriately.

The CJIS Security Policy contains thirteen separate policy and technical requirements covering numerous topics. The policy requirements include such topics as security awareness training, policy and contractual requirements. The technical requirements include such topics as establishing user access control for restricting users and the deployment of encryption to protect data in transit.

The FBI updates the CJIS Security Policy on an annual basis. These updates ensure that the policy reflects best cyber-security practices.

Agencies subject to the CJIS Security Policy receive audits with a frequency of at least once every three years. These audits determine if agencies meet the requirements of the CJIS Security Policy. This paper will focus on the requirements to encrypt CJI in transit.

Why encrypting CJI in transit is so important and what does the Security Policy require?

The main focus of the Security Policy is 'to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit'.

'to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit'. While there are various references to 'encryption' throughout, the main section where the requirements are set out is in **Policy Area 10 (Systems and Communications Protection and Information Integrity)**.

Section 5.10.1.2.1 states:

"When **CJI is transmitted outside the boundary** of the physically secure location, the data shall be immediately **protected via encryption**. When encryption is employed, 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."

It is useful to break this down into sections to fully understand what it being asked for here.

"**CJI is transmitted outside the boundary**"

When CJI leaves the LAN edge, then it is 'transmitted outside the boundary'.

One example would be CJI sent from Police Headquarters (Location 1) to its dispatch center (Location 2).

Another example would be from an agency's datacenter (Location 1) to its disaster recovery site.

Anytime data is sent across a Wide Area Network from one secure location to another it falls under the definition of 'outside the boundary'.

One common misconception is that the requirement to encrypt data in transit does not apply if an agency owns its own private fiber and only shares CJI from one location to another of the same agency.

This is simply not true and has been the reason for many agencies failing their CJIS audit.

"Protected via encryption … FIPS 140-2 certified"

Agencies are not at liberty to deploy any type of encryption they may choose. Instead they must use encryption products that meet Federal standards as set by NIST. These standards are defined in the FIPS 140-2 specification. Anytime that an agency selects encryption the chosen product must meet this standard. A common cause for failing CJIS audits is the deployment of encryption that is not certified.

Agencies should beware of a vendor claiming to have a 'FIPS complaint product' (as opposed to 'certified').

This is not just a case of semantics: the term 'compliant' means that a vendor is merely making a statement that they believe their product meets the standards set out in the FIPS 140-2 publication.

This self-assessment will not help an agency pass a CJIS audit. An agency will need to demonstrate that the encryption solution deployed is 'certified' by evidence of a FIPS certificate being issued by NIST. Agencies can verify if a vendors product has a certificate (or is currently undertaking the certification process) on NIST's website.

The importance of key management

So far we have focused on the encryption requirements spelled out by the security policy. In Appendix G, best practices for key management are set out. Agencies are strongly recommended to 'develop policies and procedures define and monitor the administrative tasks involved with protection, storage, organization, access controls and the lifecycle management of encryption keys'. This section notes that encryption keys should not be accessed by any third party and that processes should 'ensure only authorized users have access to encryption keys'.

Agencies using an encryption solution that depends on a third party service provider or carrier to manage their encryption keys should consider how this aligns to the best practices recommend in Appendix G.

The Challenges of Securing Data in Transit

Few would argue with the notion that securing data in transit is very challenging. In fact, the CJIS Security Policy appears to be sensitive to this given the lower standards required to encrypt data at rest as opposed to data in transit: a minimum key strength of 256 bit is required to encrypt data at rest as opposed the minimum of 128 bit required for data in transit encryption.

The FIPS 140-2 certification requirement for an encryption solution narrows down the pool of available options for agencies. The common choices available to agencies are: Layer 2 Ethernet based encryption; Layer 3 IPSec or purpose-built security appliances. Implementing such solutions can result in various challenges and pain points for agencies' IT departments.

Whilst such challenges vary according to products used and the type of network infrastructure an agency has in place, typical challenges arising are: initial deployment is complex, costly and time consuming requiring significant resources. These resources are required to make necessary network and configuration changes to implement the solution. Further, implementing protocols such as IP Sec as a solution, can 'blind' the networks team from knowing the type of traffic being encrypted, making their day-to-day operations more difficult.

In summary, many agencies lack resources with the requisite technical expertise to deploy an encryption solution and many are budget constrained. However, compliance with the requirement to encrypt CJI in transit is mandatory. If an agency fails to do this, then not only will it be a vulnerable target for nation state actors to exploit when attempting to breach Criminal Justice Information, but the agency also risks being denied access to CJIS Services following a failed audit. The challenge must therefore be overcome.

Overcoming the Challenges

The challenges and pain points explained above arise from the fact that the current security model used by many agencies (and corporations worldwide!) has some fundamental flaws. It relies solely on firewalls, routers, switches and IDS/IPS network devices to maintain security for data in transit. In the service networks of today, data in motion may transit many networks, both local and remote, across critical junction points that can change without notice and are untrusted. Security is no longer an abstracted network function but a vital business function that requires careful, precise planning, efficient implementation and highly visible and efficient operation.

The modern Security model must work independently of the network and without impact to the network functions by overlaying the network infrastructure seamlessly. This will allow for transparency of the network and allow for the security to react, plan and implement changes as needed.

How Certes can help law enforcement and non-CJA agencies

As discussed, there are critical challenges that need to overcome for an agency to be compliant with CJIS Security Policy. The Certes Network solution can address the following challenges:

- **CHALLENGE #1**: Ensuring CJI transmitted outside the boundary is protected via FIPS 140-2 certified encryption.

  Certes range of enforcement appliances provide FIPS certified encryption for data in transit.

- **CHALLENGE #2:** Ensuring the encryption solution provides "key strength of at least 128 bit strength"

  Certes solution provides encryption key strength of 128 and 256 bits.

- **CHALLENGE #3:** "...ensure only authorized users have access to encryption keys..."

  Certes solution provides a secure roll based management system that only allows authorized access to security policies and the associated encryption keys. Further, encryption keys are rotated per policy at the interval prescribed by the authorized user.

- **CHALLENGE #4:** Initial deployment is complex, costly and time consuming requiring significant resources

  Certes has a solution that divorces security from network infrastructure. Certes uses a universal security overlay that is agnostic to the network that eliminates the cost, complexity, and risk of maintaining independent security policy and business rules for each and every network, transport, application, and user across the enterprise.

- **CHALLENGE #5:** Standard solutions, can 'blind' the networks team from knowing the type of traffic being encrypted, making their day-to-day operations more difficult.

  In Certes patented Layer 4 solution, only the payload of the packet is encrypted. Therefore, the solution provides a transparent security overlay that protects the vital data in transit while preserving network information for use by the network devices for critical services and troubleshooting.

The challenges presented in this paper represent the most common challenges facing CJIS agencies today. However, all customer challenges are unique. For a free consultation to further examine your agency's individual requirements please our team at **sales@certesnetworks.com** or at **877.878.6655(US)**.

About Certes Networks

Certes Networks Zero Trust Security solutions protect data and applications in motion with a range of software defined security solutions. Our Zero Trust framework protects application traffic over any environment to any user, device or location; all this without affecting network or application performance whatsoever. Our patented and industry leading layer 4 stealth encryption solution gives you “Encryption without Compromise”.

For more information visit **CertesNetworks.com**

Global Headquarters
300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: +1(888) 833-1142
Fax: +1(412)262-2574
CertesNetworks.com

North America Sales
sales@certesnetworks.com

Government Sales
sales@certesnetworks.com

Asia-Pacific Sales
apac@certesnetworks.com

Central & Latin America Sales
sales@certesnetworks.com

Europe, Middle East & Africa Sales
emea@certesnetworks.com

V1-12-18-2018