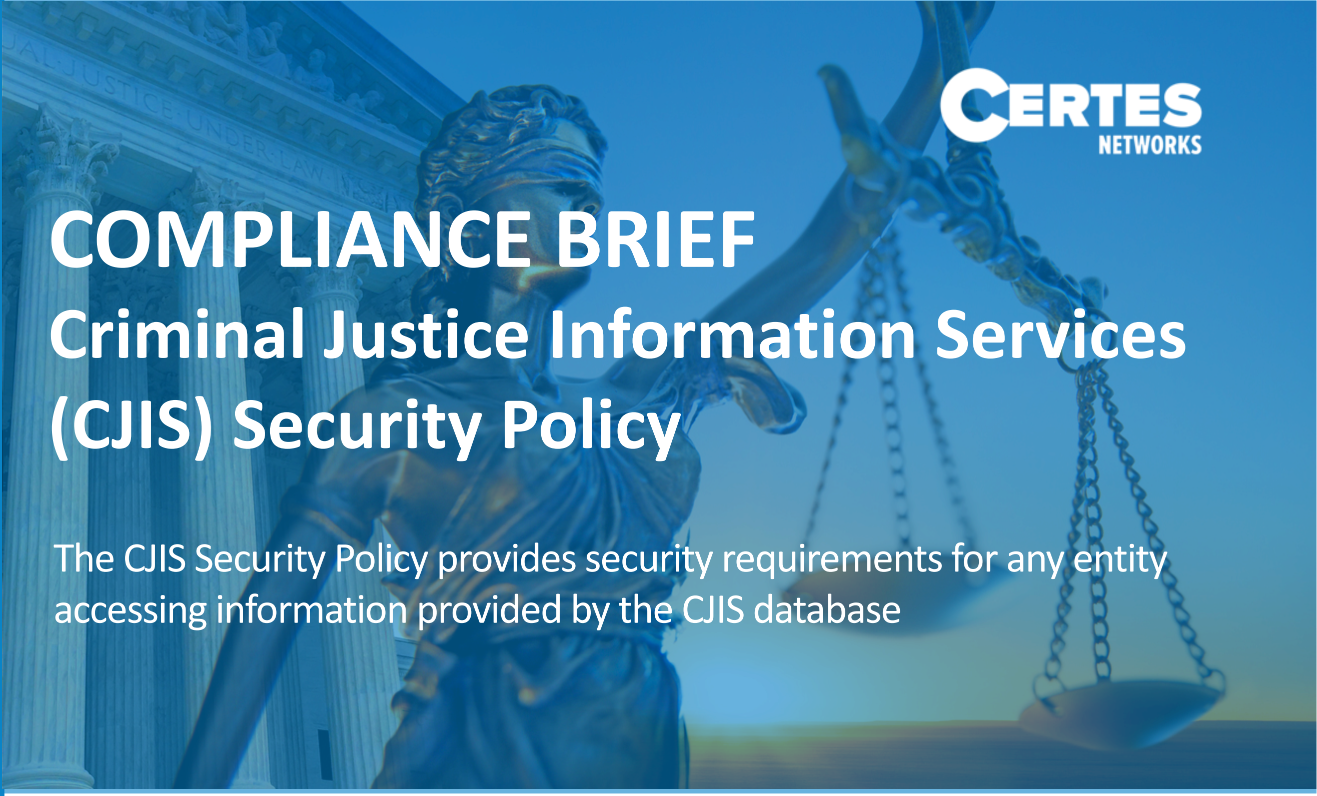

CERTES NETWORKS

# COMPLIANCE BRIEF

# Criminal Justice Information Services (CJIS) Security Policy

The CJIS Security Policy provides security requirements for any entity accessing information provided by the CJIS database

## What is the CJIS Security Policy and Why Is It Important?

Compliance with the CJIS Security Policy is mandatory for any organization that handles Criminal Justice Information.

The purpose of the CJIS Security Policy is to provide a minimum set of security requirements that must be adopted by any ***U.S. government, criminal and law enforcement agency*** that accesses the services provided by the CJIS division database.

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 every three years. These audits determine if agencies meet the requirements of the CJIS Security Policy.

## WHAT AGENCIES NEED TO KNOW

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’.

The use of encryption is fundamental to achieving this. Failure to meet requirements to encrypt data in transit has historically been a reason for agencies failing audits. Section 5.10.1.2.1 of the CJIS Security Policy sets out the requirements for encrypting CJI in Transit.

“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 these requirements.

## Main reasons for failed audits

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.

## FIPS 140-2 certified specifications

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 vendor’s product has a certificate (or is currently undertaking the certification process) on NIST’s website.

## CIVIL PENALTES

Failure to comply with the CJIS Security Policy can result in an agency being denied access to the FBI’S CJIS Database.

## WHAT SHOULD YOU DO NEXT?

Agencies should carry out an internal audit of their data governance processes to ensure that any CJI being accessed, stored or shared meets the strict encryption requirements set out at Section 5.10.1.2.1 of the CJIS Security Policy. Agencies should ensure that any encryption vendor they work with has a valid FIP 140-2 Certificate in place for any product that is to be deployed.

A copy of the CJIS Policy can be found here: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

We offer an encryption solution that is simple, scalable and uncomplicated.