CERTES
NETWORKS

TECHNOLOGY SOUNDBITE

Completing the CJIS Checklist

Law enforcement agencies are a vulnerable target and sensitive data cannot be unprotected

Author: Simon Hill, Legal & Compliance Director, Certes Networks

The Criminal Justice Information Services (CJIS) Security Policy sets minimum security requirements for any organization accessing, transmitting or creating criminal justice information (CJI). These CJIS requirements are mandated for all US local, state and federal agencies in criminal justice and law enforcement. The FBI Security Policy states that organizations under this mandate must use multi-factor authentication as a key policy area on their CJIS checklist, along with data encryption.

Agencies are a vulnerable target, essentially representing a front door for nation state actors to gain access to FBI and other federal, state, and local information shared across public safety agencies in the US. Therefore, if an agency isn't compliant with the CJIS Security Policy, it can put both law enforcement officers and the public at risk.

Passport numbers, biometric data, identity data and case/incident history are just a handful of the types of sensitive data being transferred between judicial agencies that is vulnerable to being hacked every day. The multiple, disparate locations that need to access this sensitive data adds another layer of complexity. For example, a County Sheriff's office may to need to safely transmit CJIS data implemented without having to disrupt, move or replace the current network infrastructure and it is essential to fulfil the CJIS requirement to encrypt data transmitted outside the boundary. Moreover, it is simple, uncomplicated and cost-effective.

Organizations in the law enforcement community must know what CJI data they hold, where it is being held and what measures are in place to keep it secure. With so much at stake, the time to begin securing CJI is now and it all starts with implementing encryption to adhere to the standards set out by the FBI. No organization wants to risk failing their next audit. Put simply: being CJIS compliant isn't something you can choose, it's the law.

Being CJIS compliant is of paramount importance, but many agencies and federal departments believe that deploying and maintaining encryption is too time consuming, complex and costly. Furthermore, these organizations have limited resources and budgets, so require a simple and uncomplicated management solution that would not burden their staff or be too expensive.

Removing Complexity

In reality though, it is not complicated to comply with the CJIS Security Policy. One of the key requirements of CJIS compliance is that all data being transmitted outside the boundary of a physically secure location – even if it's between two offices of the same judicial agency – must be encrypted.

This can be as simple as deploying FIPS 140-2 validated encryption technology, which is essential for government/federal organizations, subsidiaries and contractors that deal with information protected by federal government rules. Delivering security products that have been tested and validated against these rigorous standards is critical to help state and local agencies comply with data protection regulations. This technology can be implemented without having to disrupt, move or replace the current network infrastructure and it is essential to fulfil the CJIS requirement to encrypt data transmitted outside the boundary. Moreover, it is simple, uncomplicated and cost-effective.

Organizations in the law enforcement community must know what CJI data they hold, where it is being held and what measures are in place to keep it secure. With so much at stake, the time to begin securing CJI is now and it all starts with implementing encryption to adhere to the standards set out by the FBI. No organization wants to risk failing their next audit. Put simply: being CJIS compliant isn't something you can choose, it's the law.

CERTES
NETWORKS

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1(888) 833-1142
Fax: 1(412)262-2574

info@certesnetworks.com
sales@certesnetworks.com

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