FBI CJIS Security Policy (CJISSECPOL)

Version 5.9.2 effective 12/07/2022

Impact on radio communications for law enforcement

Policy:

5.10.1.2.1 Encryption for 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.
NOTE: Subsequent versions of approved cryptographic modules that are under current review for
FIPS 140-2 compliancy can be used in the interim until certification is complete.
EXCEPTIONS:
1. See Sections 5.13.1.2.2 and 5.10.2.
2. Encryption shall not be required if the transmission medium meets all of the following requirements:
a. The agency owns, operates, manages, or protects the medium.
b. Medium terminates within physically secure locations at both ends with no interconnections between.
c. Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
d. Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
e. With prior approval of the CSO.

What does this mean?

The FBI CJISSECPOL aims to protect all Criminal Justice Information (CJI) and Personal Identifiable Information (PII) whenever that data is transmitted outside of a secure location. This includes voice transmission of this sensitive information. Whenever this information is transmitted outside of a physically secure location, the data must be protected with AES encryption and FIPS 140-2 security.

When does this go into effect?

This policy became effective on 12/07/2022 and became auditable at the time of publishing. Although it is in effect now, it will depend on where you are in your audit cycle from KHP CJIS as to when a KHP CJIS Auditor will examine this topic with your agency. Every agency in Kansas is on a three-year cycle and KHP (as the CJIS Systems Agency (CSA)) is on the same three-year cycle with the FBI CJIS Unit. Our last audit was 03/08/2022 and the next audit should be around March 2025.

How does this impact my operations?

Basically, to be in compliance with this portion of the SECPOL, a law enforcement agency must use an AES encrypted with FIPS 140-2 talkgroup or channel to transmit and receive CJI or PII. This can be handled by either encrypting all of your talkgroups/channels or you can dedicate one informational talkgroup/channel to run all these transactions on. This would include all driver license checks, vehicle registration checks, warrant checks and criminal history checks.

What if I am not on 800 MHZ or KSICS?

The policy does not specify radio band and is specific only to the type of data transmitted or received. This means that the policy applies if you are VHF, UHF or 7/800 MHz

Are there any alternative options available?

The only recognized exemptions to this policy are the use of a mobile data terminal (in-car computer MDT/MDC), cell phone or fax machine. While some agencies may be able to switch to strictly running all this type of traffic through their computer, this option is likely not a complete solution if operating outside your vehicle. You might also be considering using a cell phone; however, FBI CJIS specifies the cellular device must be agency owned and many agencies do not issue cell phones, or a cell phone may not be the most tactical and safe device to operate on during a citizen interaction. Fax machines don’t really apply unless you are in an office environment.

What is the CSA’s stance on this policy?

KHP CJIS Auditors will use this time (before our next FBI CJIS Audit) to educate agencies on the new policy but will not list it as a violation. Once we go through our next FBI CJIS audit, we should have a better understanding of how they will enforce the policy and if any subsequent sanctions may be involved. This will steer how we (KHP CJIS) audit our law enforcement partners.

Does this affect Fire or EMS?

The FBI CJIS SECPOL does not govern anyone other than law enforcement and does not apply or affect anyone else.

03/21/2023