From Dep. Chief Houston:

Anthony PD radio presentation-

1. Currently the KBI and KCJIS or Kansas Criminal Justice Information Sharing is mandated that any users on the State P25, 700/800 MHz system has to be compliant as of **January 1st, 2024.** We are currently out of compliance currently using the State owned and operated P25 system. Requirements include AES encryption on all used channels, we have two, Law 1 and Tac 1, Phase II P25, Multi-Key and AES encryption, and OTAR or Over the Air Rekeying capability. We currently use Phase I non-encrypted radios which are not capable of being programmed to Phase II nor encrypted capable. (See mandate)
2. Currently the Director of Harper County Communications/ Emergency Management, Chirs Cintron, says even though we are currently not in compliance, the state will not enforce this change until we have a local audit. She believes this audit will occur around the first of 2025.
3. Encryption is key due to law enforcement running personal information over the air, i.e. driver's licenses, criminal history, etc.
4. If not compliant, we could ultimately be kicked off the state system.
5. **Second issue---**
6. Anthony and Harper are in low areas, and we currently are bouncing off two state towers, Barber County and Sumner County.
7. We have 85-90% dead areas where portable or handheld radios will not communicate with dispatch or other officers unless we are inside our patrol vehicles using mobile, higher-powered radios. (Currently and has been a huge officer safety issue).
8. The new Phase II radios have two options, one being a Wi-Fi capable/ LMR "land mobile radio" which LMR is the state tower 700/800 MHz or LTE "cellular"/ LMR radio. Wi-Fi capable handhelds would require expanding our cellular data package with Verizon to include mobile hotspots that we would have to carry on our bodies when exiting the vehicles due to poor range along with the radio when the signal cannot reach the state tower. The LTE/LMR radios are more expensive however the package plan includes 7 years of LTE. (See both quotes). This will resolve dead spot issues, if LTE plan chosen, county would not have to get additional tower in Harper County. A tech with First wireless, (old Mobile Radio) tested the LTE version in Harper County and when signal from LMR was not capable or insufficient it switched to LTE (cellular) seamlessly.
9. Cintron presented the county commissioners last year to have a state tower installed, which is a multi-million-dollar venture with grant funding availability last year, however the plan was denied. A new tower would have solved the issue of radio signal problems; however, it will not fix the new mandate from KCJIS, which is left to every individual department in Harper County.

10. Currently a new FEMA grant has become available and one in September, (Edward Byrne JAG) that would hopefully aid in the radio costs. Wi-Fi plan without the additional expense of the hotspot x2 and unlimited data service on the two hotspot is slightly over $40,000, the LTE version with 7 years of LTE is slightly over $62,000. Grant seeking and application if permitted could help offset costs. The current FEMA grant deadline is 06/24/2024.
11. After speaking with an associate of First Wireless, if Grant availability fails, they partner with a lease program, (Lease Corporation of America), although stated there are interest rates and suggested using local banks to lower the interest rates.

Dwight D. Eisenhower State Office Building
700 S.W. Harrison Street
Topeka, KS 66603-3745
Julie L. Lorenz, Secretary
Robert Fuller, P.E., Chief

Kansas
Department of Transportation
Bureau of Maintenance

Phone: 785-296-3576
Fax: 785-296-6944
kdot#publicinfo@ks.gov
http://www.ksdot.org
Laura Kelly, Governor

KSICS Encryption Requirements

The below requirements are for ALL Talk-groups associated with KSICS.

1: ALL talk-groups WILL be assigned in the MSO as Clear or Secure on July 1st, 2024
2: ALL encrypted Talk-groups must be aligned with the state Encryption Template by Jan 1st, 2024
3: Regional AES Talk-Groups will be strapped Encrypted only.
4: Existing Encrypted Talk-Groups can be ADP, DES or AES.
5: State Interoperability CKR/SLN 1-8 will be deactivated on Jan 1st, 2024
6: ALL Talk-groups on KSICS will be marked in the system as in the clear only unless talk-group and CKR are provided to the KSICS administrator **Effective Jan 1st, 2024**
7: ALL Key ID's must align with authorized CKR/SLN's by Jan 1st, 2024
8: ALL New CKR/SLN will be assigned through initial Talk-Group requests.
9: ALL New Encrypted Talk-Groups will be AES only to include all W.A.V.E Talk-Groups.
10: Existing encrypted Talk-group owners will need to Contact: KSICS_Encryption@ks.gov KDOT's program administrator for CKR/SLN assignments and or verification of the State Encryption template alignment prior to Jan 1st, 2024
11: All KVL's must be registered with KSICS MSO Administrator, Serial Number, Model, POC, and physical location. Contact KSICS_Encryption@ks.gov
12: ALL Key information will NOT be shared or transferred without prior written approval by JHA (Jurisdiction Having Authority)
13: ALL MCC 7500E Consoles must have a Cryptor to be active on KSICS (no soft key)

Note: This requirement has been established to meet the encryption interoperability needs for public safety, allow the seamless transition for capacity needs via Phase 2 TDMA upgrades if needed, and provides a guarantee to the purchasing party that the device will operate to meet the needs of public safety via the P-25 CAP program.
Please notify the KSICS Administrator as soon as possible if you are currently using "selectable encryption" (meaning you can switch to encrypted traffic on the same normally clear talkgroup) on any talkgroup ID that is assigned to your agency. Failure to notify the KSICS Administrator prior to Jan 1st, 2024, may result in operational issues for your agency communications. If an agency does not change CKR/KID's by Jan 1st, 2024, your agency could face operation issues with your LMR communications. These required changes are necessary for the whole radio community, and it is each agencies responsibility to ensure corrections are made prior to the Jan 1st, 2024 deadline.

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.

Is this the same thing as the new KDOT requirements for KSICS (Statewide Radio System)?

No, this new requirement is from FBI CJIS and is not the same, although it does work in conjunction with KDOT's effort to ensure radios purchased and placed on the system after January 1st, 2024 have the capability for multi-key AES encryption for public safety agencies.

Does the FBI CJIS requirement have the same timeline of January 1st, 2024 as the KDOT requirements?

No, because it is not same requirements and KDOT requirements affect all public safety and not law enforcement only like the FBI CJIS SECPOL. The KDOT requirements are for how the radio is required to be equipped with features and how it operates on the state system only.

What are the new KDOT Statewide Radio System requirements?

Dwight D. Eisenhower State Office Building
700 S.W. Harrison Street
Topeka, KS 66603-3745
Julie L. Lorenz, Secretary

Kansas
Department of Transportation
Office of the Secretary

Phone: 785-296-3461
Fax: 785-368-7415
kdot#publicinfo@ks.gov
http://www.ksdot.org
Laura Kelly, Governor

KSICS New User Device Requirements

The Kansas Department of Transportation requires that any radio purchased for Public Safety use on the State of Kansas P25 radio system must be capable of the following feature:

1 Approved by P25 Compliance Assessment Program (CAP)
2 P25 Phase 2
3 700/800 MHz
4 Multi-Key
5 AES Encryption
6 Over the Air Rekeying (OTAR)

The radios do not need to be ordered with these features installed but must be capable of programming them into the them later.

This requirement will be effective beginning January 1, 2024