Radio Traffic Encryption

This document clarifies FBI Criminal Justice Information Services (CJIS) Security Policy requirements for encrypting radio traffic that contains FBI criminal justice information (CJI) while maintaining a high level of interoperability for radio communications to protect the safety of responders.

The FBI encryption requirement applies only if FBI CJI is being communicated. It does not require that a law enforcement main or county main be encrypted. It may require that agencies use an alternate talkgroup or other means of transmitting CJI.

The requirement should never compromise responder safety. While the Minnesota Bureau of Criminal Apprehension (BCA), as the FBI CJIS Systems Agency (CSA) for Minnesota, is responsible for ensuring that agencies are aware of and comply with FBI CJIS Security Policy requirements, agencies unable to comply with the encryption requirement in a critical situation will not face sanctions. FBI CJIS Security Policy section 5.13.1 requires that land mobile radio (LMR) communications that contain FBI CJI be encrypted. The BCA CJDN Security Policy clarifies the FBI requirement, stating that the encryption must be NIST-certified FIPS 140-2 compliant and use at least a 128-bit symmetric key.

The Statewide Emergency Communications Board (SECB) is working with agencies and advisory bodies on how to best move forward on building a plan to operationalize these requirements while maintaining a high level of interoperability for communications. While agencies may be found out of compliance during an audit by the FBI, the BCA will work with agencies to develop a plan for coming into compliance.

As long as agencies have a compliance plan, no sanctions will be implemented.

Below are answers to frequent questions about the requirement, including what data is considered to be CJI.

Frequently Asked Questions

Does all radio traffic need to be encrypted?

No. Only radio traffic that contains FBI CJI must be encrypted.

Can EMS, fire and public safety entities utilize law enforcement “Main” talkgroups?

Yes, EMS, fire, and public safety entities can utilize law enforcement "main" talkgroups, but careful consideration must be given to how CJI may be relayed to law enforcement only. FBI CJI must not be transmitted on that shared talkgroup.

Additional note: If the "main" talkgroup includes non-law enforcement agencies, all FBI CJI must be communicated using a different method, such as a separate talkgroup designated for law enforcement use only that is encrypted in compliance with FBI CJIS Security Policy, or using cell phone or Mobile Data Terminal (MDT). FBI CJIS Security Policy section 5.13.1.2.2 exempts cell phone traffic from the encryption requirement.

Transmitting FBI CJI on an ARMER talkgroup that is encrypted with DES-OFB or ADP does not meet the FBI requirement. A talkgroup must use Advanced Encryption Standard (AES) encryption to meet FBI CJIS Security Policy requirements.

What information is considered to be FBI CJI?

The FBI defines CJI as data from FBI CJIS systems that are necessary for law enforcement and civil agencies to perform their missions including, but not limited to, the following data: biometrics, identity history, biographic, property, and case/incident history. This includes data from the FBI's Interstate Identification Index (III), which is criminal history or biometric data, and the National Crime Information Center (NCIC), which includes hot files such as Wanted Person File, Vehicle File, Missing Person File, etc. This requirement does not apply to data generated from local agency systems. It also does not include data from BCA systems, unless that data originated from an FBI CJIS system.

What are some specific examples of information that the FBI requires to be transmitted via encrypted ARMER talkgroups?

The following files from NCIC may only be transmitted via encrypted talkgroups: Gang File, Known or Appropriately Suspected Terrorist File, Convicted Persons on Supervised Release File, National Sex Offender Registry, Historical Protection Order File, Identity Theft File, Protective Interest File, Missing Person File, Violent Person File, NICS Denied Transaction File, Immigration Violator File, Originating Agency Identifier (ORI) File, Interstate Identification Index (III) File, Article File, Gun File, Boat File, Securities File, Vehicle File, Vehicle/Boat Pat File, Image File, License Plate File, Unidentified Person File, Foreign Fugitive File and Wanted Person File.

The requirement also applies to information from BCA systems that contain or may contain FBI CJI, such as the Automated License Plate Reader (ALPR) Data File, Domestic Abuse No Contact Orders (DANCO), Orders for Protection (OFP), Harassment Restraining Orders (HRO), Keep Our Police Safe (KOPS) files, Predatory Offender Registry Electronic Submission (POR ES), Criminal History System (CHS), and the POR Law Enforcement (POR LE) website.

What are some specific examples of information that the FBI does not require to be transmitted via encrypted ARMER talk groups?

The FBI requirement does not apply to information from BCA systems which does not originate from FBI CJIS systems. Data from DVS Access, eCharging (DWI, Citations, Complaints, Incident Referrals, and Search Warrants), Livescan Message Enhancement (LME), Minnesota hot files that do not contain FBI data (Arrest

Warrant Index and Minnesota Criminal Gang Investigative Data System), Minnesota Repository of Arrest Photos (MRAP), National Incident Based Reporting System (NIBRS) data, Permit Tracking System (PTS), and Vehicle Impound Data. The requirement also does not apply to data that originates from local agencies. Minnesota state law governs the dissemination of this data.

Are both "restricted" and "non-restricted" NCIC files required to be encrypted?

Yes. Information from any NCIC file must be encrypted if it is transmitted outside a physically secure location, regardless of whether it is restricted. The difference between "restricted" and "non-restricted" NCIC files is what law governs their use. U.S. Title 28 CFR Part 20 governs NCIC files. Non-restricted files may be used for any purpose consistent with an agency's responsibilities. Agencies should check with their legal counsel or data practices expert for guidance on authorized uses of NCIC non-restricted files.

Why does the FBI require some information to be encrypted when the same information can be made publicly available by my agency?

The FBI requirement applies only to data that is queried from FBI CJIS systems. Please see the definition of FBI CJI above. When the same type of data originates from a law enforcement agency in Minnesota, Minnesota Statutes, Chapter 13 governs the availability of that data. Your agency's legal counsel or data practices expert can provide guidance related to Minnesota data practices law.

Does this mean that radio recording in the PSAP logging equipment also need to be encrypted?

Yes. Any radio traffic that contains FBI CJI must be encrypted in transit and at rest at any time it is outside of a physically secure area, as defined in the FBI CJIS Security Policy. Encryption in transit must use NIST certified FIPS 140-2 compliant encryption and encryption at rest must use either NIST certified FIPS 197 or FIPS 140-2 encryption.

What are other states doing to meet this requirement?

Most states are encrypting law enforcement radio traffic in at least some agencies and at least two states have mandated compliance with the FBI CJIS Security Policy encryption requirement. The SECB can provide more information about what other states are doing.

- The North Dakota Office of Attorney General Bureau of Criminal Investigation published a memo in January 2020 requiring all CJI communicated over a radio system to be encrypted in accordance with the FBI CJIS Security Policy (radio-encryption-requirement-memo.pdf) and in September 2020 published a standard to establish policy and procedures for the encryption of CJI on North Dakota's Statewide Interoperability Radio Network (SIRN) (https://www.ndit.nd.gov/sites/www/files/documents/technology-section/siec/2-2-0-law-cji-encryption.pdf).
- The California Department of Justice in October 2020 notified state law enforcement agencies of a requirement to encrypt any radio communications with CJI or Personally Identifiable Information (PII).

What does this mean for agencies until they come into compliance?

The SECB is working with agencies and advisory bodies on how to best move forward with building a plan for operationalizing these requirements. While agencies may be found out of compliance during an audit by the FBI, the BCA will work with agencies to develop a plan for coming into compliance. As long as agencies have a compliance plan, no sanctions will be implemented.

What are some short term best practices that can be implemented to mitigate potential violations of the encryption requirement while agencies work toward a long-term solution?

Move your FBI CJI radio traffic to a separate encrypted talkgroup that only law enforcement can access (information or "data" talkgroup), or relay information via cell phone or Mobile Data Terminal (MDT).

For additional information

Contact the State Program Coordinator for Minnesota Land Mobile Radio, Marcus Bruning, at marcus.bruning@state.mn.us, or your local or regional ARMER System Administrator.