MEMORANDUM
OFFICE OF ATTORNEY GENERAL
BUREAU OF CRIMINAL INVESTIGATION

TO: Darin Anderson/NDIT Public Safety Program Manager

FROM: Rebecca Hooker/CSA Information Security Officer

RE: Radio System Encryption Requirements

DATE: January 3, 2020

The purpose of this memorandum is to clarify the CJIS security encryption requirements pertaining to Radio System communications.

According to the FBI CJIS Security Policy, communication of FBI Criminal Justice Information (CJI) shall be encrypted. The CJIS Security Policy can be found online at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

CJIS Security Policy section 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.

CJIS Security Policy section 5.13.1 - Wireless Communications Technologies:

> Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described in 5.13.1.1 - 802.11 Wireless Protocols.

Examples of CJI that could be communicated over the radio would be Wants, Warrants, Missing Persons, and any information obtained from NCIC. Should state or FBI CJIS audit findings determine an agency is utilizing a radio with no encryption to communicate CJI, that agency will not be compliant with the CJIS Security Policy. Noncompliance can result in termination of NCIC services.

If you have any questions pertaining to the CJIS Security Policy, please feel free to contact me at 328-5502, rhooker@nd.gov.

Thank you