Integrated Public Safety Commission
100 N Senate Ave., N825 Indianapolis, IN 46204

Best Practices for Encryption in 700/800 MHz Public Safety Radio Systems

Public safety radio systems operating in the 700/800MHz spectrum, like Indiana's Project Hoosier Safety Acting for Everyone-Together (SAFE-T) statewide radio network, support encryption to safeguard sensitive communications and maintain operational security.

This document outlines best practices that agencies must follow for the effective planning, implementation, support and maintenance of encryption on the SAFE-T radio network.

1. Understand Regulatory Requirements and Best Practices:

Familiarize yourself with regulatory guidelines and best practices, such as those set forth by the Federal Communications Commission (FCC) and the Cybersecurity and Infrastructure Security Agency (CISA) regarding encryption usage in public safety radio systems.

Ensure compliance with relevant regulations and best practices to avoid legal complications and maintain network integrity.

2. Choose the Right Encryption Standard:

Select encryption algorithms that meet your agency's security needs, while considering interoperability with neighboring agencies. Be sure to include existing radio feature sets in your decision; such as ADP versus AES or single-key versus multi-key capabilities.

Advanced Encryption Standard (AES) is the recommended standard on the IPSC system (as it is the Project 25 standard, 256-bit algorithim)

There are other encryption algorithims as well, including:

- Advanced Digital Privacy (ADP) - Motorola proprietary algorithim
- Rivest Cipher 4 (RC4/ARC4) - Harris proprietary algorithim
- *Digital Encryption Standard (DES) - 56 bit algorithim, not recommended by IPSC/NIST/CISA*

3. Prioritize Encryption Key Management

Establish a robust key management system to secure encryption keys. Only a very small number of people should be generating keys to maintain security.

Regularly update and rotate encryption keys to minimize vulnerabilities. Key rotation should be done at least once a year. Implement strong access controls for key management to prevent unauthorized access.

Keys should be kept in writing, secured in a safe or locked environment. Additionally, consider storing keys in a secured digital archive (such as a password vault).

Encryption keys should ***never*** be transmitted via email or other electronic means.

Integrated Public Safety Commission
100 N Senate Ave., N825 Indianapolis, IN 46204

4. Physically Secure Radio and Encryption Key Equipment:

Protect radio equipment physically and logistically to prevent theft or unauthorized tampering. Use tamper-evident seals and secure storage to safeguard devices and prevent unauthorized access to encryption settings.

When handling a Key Variable Loader (KVL), a usage log should be kept to maintain accountability.

5. Maintain Interoperability:

Coordinate encryption settings with neighboring agencies to ensure seamless communication.

All encryption Storage Location Numbers (SLN's) should be coordinated through IPSC. If you do not coordinate, you risk breaking interoperability.

Test interoperability regularly to identify and address potential issues.

6. Educate and Train Personnel:

Train personnel on the proper use of encryption features and secure communication practices.

Conduct periodic refresher training to keep users up to date on encryption protocols.

Encryption features in radios, such as specifically encrypted zones or toggle switches, should be standardized throughout your agency to prevent confusion when operating a different device.

7. Balance Security and Usability:

Strive for a balance between security/encryption and ease of use/usability. Avoid overly complex encryption configurations that may hinder quick response times during emergencies.

When setting up encryption in the radio, it is recommended that a channel/talkgroup be full-time encrypted or full-time clear.

Eliminating the use of toggle switches and button-activated encryption will help to prevent the accidental transmission of unsecured sensitive information.

8. Implement End-to-End Encryption:

Consider implementing end-to-end encryption for communications (voice and data) to ensure confidentiality and integrity.

Protect all sensitive information, including tactical plans, patient data, and criminal records.

Ensuring integrity confirms the validity of information, removing the possibility of bad actors relaying false or dangerous information.

Integrated Public Safety Commission 100 N Senate Ave., N825 Indianapolis, IN 46204

9. Monitor and Audit Encryption Usage:

Establish regular monitoring and auditing processes to detect anomalies or potential security breaches.

Review access logs and encryption key activities to maintain network integrity.

System statistics regarding encryption can be gathered by contacting the IPSC Connection Center via email at icc@ipsc.in.gov or phone at 317-234-1540

10. Plan for Encryption Key Recovery:

Develop a key recovery plan to gain access to encrypted data in case of key loss or unforeseen emergencies.

Ensure that key recovery procedures are secure and well-documented. One potential option is maintaining a backup Key Variable Loader (KVL) or key management database to ensure keys are not lost if a device or storage method becomes unavailable.

Encryption is a critical component of 700/800MHz public safety radio systems, ensuring the confidentiality, integrity, and security of sensitive communications.

By following these best practices, public safety agencies can enhance their encryption strategies, maintain regulatory compliance, and effectively protect their communications during critical incidents. Balancing security measures with operational needs is key to ensuring the continued success of these vital systems.

Additional Encryption Resources:

Regulations:

- Code of Federal Regulations Title 47, Chapter I, Subchapter D, Part 90, Subpart R, 90.553 - Encryption
- Federal Communications Commission (FCC) - 16-111

Best Practices/Other Documents:

- Cybersecurity and Infrastructure Services Agency (CISA) and SAFECOM - Encryption Resources Website
- CISA/FPIC/P25 Project - The Who, What, When, Where, How, and Why of Encryption in P25 Land Mobile Radio Systems
- SAFECOM/FPIC/NCSWIC - Operational Best Practices for Encryption Key Management
- SAFECOM/FPIC/NCSWIC - Encryption Key Management Fact Sheet
- SAFECOM/FPIC/NCSWIC – Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems - Developing Methods to Improve Encrypted Interoperability in Public Safety (Fact Sheet)

Questions Regarding Encryption?

Please contact the IPSC Connection Center at icc@ipsc.in.gov or 317-234-1540