OPERATIONAL BEST PRACTICES FOR ENCRYPTION KEY MANAGEMENT

AUGUST 2020

Federal Partnership for Interoperable Communications
SAFECOM/National Council of Statewide Interoperability Coordinators

PREFACE

In coordination with SAFECOM and the National Council of Statewide Interoperability Coordinators, the Federal Partnership for Interoperable Communications (FPIC) continues to provide public safety officials and agencies with the information necessary to make informed decisions when implementing encryption in public safety communication systems.

This document is the fourth in a series of documents informing public safety on encryption. The first document, *Considerations for Encryption in Public Safety Radio Systems*, described agency requirements related to land mobile radio (LMR) encryption. It outlined the types of radio traffic that should be considered for encryption, including sensitive law enforcement information, personally identifiable information, tactical/investigative communications, time-sensitive disaster/incident response information, and other communications that can impact the safety of public safety personnel and the public.

The second document, *Guidelines for Encryption in Land Mobile Radio Systems*, addressed encryption methodology—the strategy for determining which encryption method or algorithm best protects sensitive information. It identified considerations that should be included in any evaluation of encryption solutions as well as pitfalls to avoid.

The third document, *Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems*, provided an overview of encryption key management related to Project 25 LMR systems, with an emphasis on practices that public safety agencies have found to be most helpful in effectively managing encryption both within their agencies and with their mutual aid partners.

For more detailed information on the content of the three previous documents, refer to their respective fact sheets in **Appendix D**.

This document—*Operational Best Practices for Encryption Key Management*—continues the education efforts. This document thoroughly explores encryption challenges relevant to public safety LMR systems and provides the public safety community with specific encryption key management best practices and case studies that illustrate the importance of secure communications.

The *Operational Best Practices for Encryption Key Management* document was developed in partnership with the National Law Enforcement Communications Center (NLECC), the National Institute of Standards and Technology, and subject matter experts from federal, state, and local agencies.

TABLE OF CONTENTS

INTRODUCTION

The public safety community must protect critical information and sensitive data, particularly within land mobile radio (LMR) communications. Standard compliant encryption is the most effective method to ensure that information cannot be intercepted or compromised. Encryption uses an algorithm (a set of computer instructions) to encode voice and data transmissions in such a way that only authorized personnel with properly equipped radios can decode and understand those transmissions. The algorithm generates a random string of bits, called an encryption key, that enables the sender to encode a transmission and the receiver to decode it. Effective encryption relies on keeping encryption keys secret and secure.

While encryption can provide needed protection, rapid advances in technology have compromised some encryption methods. At the same time, inconsistent and careless encryption key management will make even the most securely encrypted LMR system vulnerable. This document is a resource for agencies to establish policies and practices for secure encryption management. It does not mandate the use of encryption; it is intended solely to provide guidance through actual practitioner experience. Further, it outlines the risks and benefits involved in key management practices and techniques.

Agencies planning to implement encryption in their LMR systems should contact their Statewide Interoperability Coordinator (SWIC) for further information and resources specific to their state or region.

According to the Federal Partnership for Interoperable Communications (FPIC) Security Working Group, ***"An effective way to enhance interoperability is to develop a common set of best practices that will encourage public safety agencies to work toward a common goal of encrypted operations and interoperability. If public safety agencies subscribe to these best practices, the goal can be realized and will not interfere with an individual agency's ability to configure its encryption to meet unique needs."***

BASICS OF KEY MANAGEMENT

Public safety agencies face a broad range of options when it comes to encryption key management, including choice of encryption algorithm, various protocols for key generation, and determining cryptoperiods (the length of time between system-wide changes of encryption keys). These options can be simplified by following a number of common-sense practices developed by public safety agencies not only to protect their own systems' communications but also to maintain interoperability with their local, state, and federal mutual aid partners.

The U.S. Customs and Border Protection (CBP) National Law Enforcement Communications Center (NLECC) provides key management services to public safety agencies at all levels of government. NLECC generates and distributes national interoperability keys and unique encryption keys for individual agencies' use and maintains a database of assigned keys to prevent key overlap and conflicts among agencies.

BEST PRACTICE
Use NLECC's key management services for a reliable, uniform approach to key management and interoperability of encrypted devices.

All encryption-ready LMRs have one or more "slots" for storage of encryption keys. These slots, referred to as Storage Location Numbers (SLN), must be carefully assigned and managed to ensure interoperability among encrypted Project 25 (P25) radios. NLECC and FPIC created the National Storage Location Numbers Assignment Plan, which established a common configuration to enhance interoperability of encrypted radios nationwide. In June 2014, FPIC approved a plan to reserve SLN 1-20 for national interoperability use.

BEST PRACTICE
Adopt the National SLN Assignment Plan to coordinate encryption among interoperable radios and systems and minimize SLN and encryption key conflicts with other agencies.

The general practices listed on the following page form the basis for an effective key management program and are discussed in detail in later sections of this document. Examples of how these practices benefit agencies and the consequences of not following them can be found in the **Key Management Use Cases** section.

Basic Key Management Practices

- Identify key management authorities, roles, and responsibilities
- Utilize Project 25 standards-based encryption to maximize communications interoperability
- Develop an encryption key management plan to protect against compromise and reduce operational uncertainty
- Coordinate key management plan with partner agencies
- Maintain accountability of all key management devices
- Limit key distribution only to authorized entities
- Determine number of encryption keys needed from NLECC
- Obtain encryption keys from NLECC
- Follow key management practices recommended by NLECC
- Maintain a record of all devices that receive encryption keys
- When establishing encryption key procedures, pay close attention to National SLN 1-20 Assignment Plan (**Appendix C**)

KEY MANAGEMENT USE CASES

The need for encryption in the public safety community is increasing as technologies for monitoring public safety communications become more accessible. Scanners and smart phone apps make it easy for anyone to access sensitive law enforcement and emergency medical services (EMS) information transmitted in the clear (without encryption). At the same time, encrypting an LMR system can potentially interfere with interoperability within and among agencies if encryption protocols are not shared among users. This section presents several real-world use cases that illustrate how various agencies have overcome these and other challenges.

Case Study #1: Vulnerabilities in key transmission procedures

Encryption keys—also referred to as cryptographic keys—are distributed to agencies by NLECC through secure connections to the agencies' key fill devices (KFD). NLECC requires that any KFD to which it transmits keys must have its Wi-Fi capabilities disabled. In contrast to Wi-Fi, Over-the-Air Rekeying (OTAR) provides a secure connection to subscriber units. A KFD that has its Wi-Fi capabilities disabled is referred to as hardened. Hardening ensures that the KFD does not inadvertently "leak" the encryption keys onto a wireless network where unauthorized personnel could access them. Agencies, in turn, transmit the NLECC keys to other KFDs that are used to distribute the keys to its individual radios (a.k.a. subscriber units or SU). Unless these secondary KFDs are hardened, they are considered noncompliant and create a serious vulnerability. As shown in **Figure 1**, sharing keys over a device with active wireless connections poses a serious risk that the keys can be intercepted and creates a domino effect that can impact the entire system, as well as the systems of mutual aid partners.

BEST PRACTICE

Do not use any type of Wi-Fi enabled device to receive or share encryption keys.

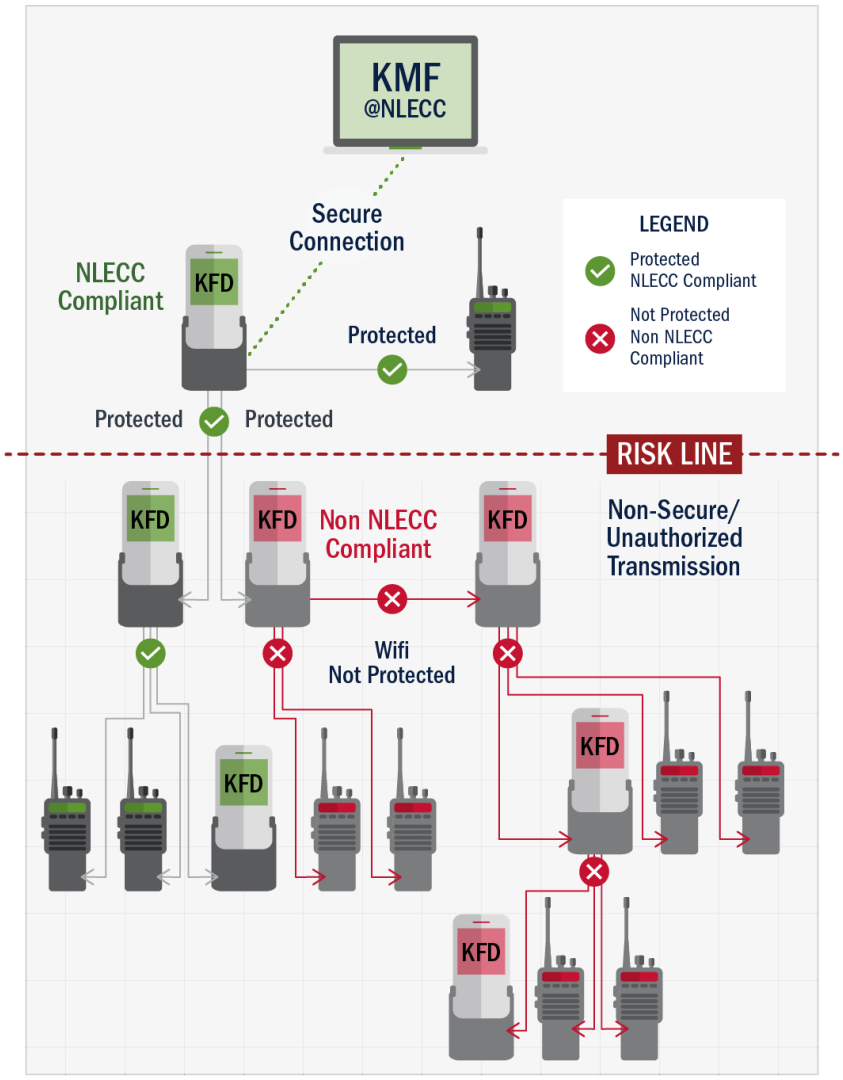


Figure 1: Security risk when a Wi-Fi enabled device is used for cryptographic key distribution

To maintain the security of an encrypted system, a system administrator must know who has access to all encrypted radios and encryption keys. Distributing cryptographic keys via wireless-enabled devices weakens the administrator's ability to keep accurate records and can disrupt the agency's and even NLECC's ability to manage keys properly. Distributing keys for short-term use during events or incidents can also create vulnerabilities if the process is not tightly managed.

BEST PRACTICE

Keep complete and accurate records of KFDs, SUs, and organizations with whom you share keys. Confirm with NLECC that those organizations are authorized to receive keys NLECC provides.

Case Study #2: Operational use of Memorandum of Understanding (MOU) and Memorandum of Agreement (MOA) interoperability agreements and informal agreements

A county sheriff's department approached the U.S. Coast Guard (USCG) about establishing encrypted communications with the agency in order to improve coordination during interagency operations. The sheriff's department had recently purchased a radio capable of being programmed with USCG very high frequency (VHF)-frequency modulation (FM) command and control channels, as well as having Advanced Encryption Standard (AES) encryption. The Coast Guard provided the necessary channel programming information and arranged to provide interoperable encryption keys on an annual basis. Because this was a long-term interoperability initiative, it required a formal agreement, and an MOA was drawn up to document each party's key management roles, responsibilities, and processes. The MOA enabled the sheriff's department to have consistent, direct, encrypted communications with the Coast Guard and clearly defined each organization's obligations, which provided legal protections for both agencies.

In another instance, a joint state/federal task force planned to serve arrest warrants to several dozen individuals over the course of a few hours. The plan required close coordination and, of course, encrypted interoperable communications among hundreds of local, state, and federal law enforcement officers, many of whom had never worked together. Because the operation was a one-time event and there was insufficient time to draft an MOA or MOU, the technical staffs of the various agencies developed an informal interoperability agreement through e-mail and phone calls to resolve the various technical challenges and support a successful operation.

BEST PRACTICE

For interagency operations requiring encrypted interoperable communications, participating organizations should implement MOUs/MOAs when practical to formalize key management and governance processes. Where circumstances do not allow for formal agreements, organizations should agree informally on roles and responsibilities but be certain there is clear understanding among them.

Case Study #3: Reporting of lost/stolen devices

A local law enforcement agency was puzzled by a sudden decrease in apprehensions during an ongoing drug operation and suspected its encrypted communications were being intercepted. A confidential informant revealed that an agency LMR had been stolen and the criminals were using it to eavesdrop on the agency's investigative and tactical communications. Once the key compromise was discovered, the agency remotely disabled the stolen radio and immediately changed the encryption keys in all agency devices. Drug seizures and apprehensions noticeably increased.

The loss or theft of a hand-held radio can seriously compromise public safety operations. During radio training, all public safety personnel must be made to understand that reporting a missing LMR immediately is paramount. System administrators must report to NLECC the loss of any radio that has NLECC cryptographic keys.

BEST PRACTICE

Require all personnel to promptly report lost and stolen radios to minimize the risk to the agency's communications. Report to NLECC the loss of any radio containing one or more NLECC encryption keys.

Case Study #4: Not maintaining control of key fill devices

A municipality saw a gradual increase in drug trafficking and related crime, but investigators found themselves thwarted when trying to make arrests. Eventually they discovered that the criminals had identified a radio shop employee who had one of the municipality's KFDs, which he used to load keys onto agency radios. The criminals paid the employee to load a cache of their radios with the cryptographic keys and so were able to monitor the narcotics force's encrypted communications and had prior knowledge of planned raids and other operations.

BEST PRACTICE

Key administrators should maintain accountability and security of all KFDs. If third parties are entrusted with KFDs to load keys into agency radios, those parties should be thoroughly vetted and carefully monitored.

Case Study #5: Use of standardized encryption protocols and coordination among partner agencies

A department of health emergency medical services (EMS) division realized that the addresses and patient information of some of the county's celebrity residents could be at risk of public release. As a precaution, they switched all paramedic-hospital communications to a P25, AES 256-bit encrypted, trunked radio system operated by the county. The EMS agency licenses 47 emergency medical Advanced Life Support (ALS) providers for ALS radio contact. The providers include fire departments, private ambulance companies, sheriff special weapons teams, and aero-medical services. In addition, 16 base hospitals interface with the field units. Key management was assigned to the sheriff's department, which now determines which keys will be utilized and the OTAR schedule for all radios.

The sheriff's department shares the information at the monthly EMS agency/stakeholder meetings. The date and time of OTAR events is shared at least two months in advance to give each stakeholder time to plan for updating. The time of day (usually early morning before the daily paramedic-hospital radio check[1]) is chosen to enable radio users to make sure the OTAR is successful ahead of the day's operations. Agencies that do not have OTAR-capable radios are given additional time to have their radios physically rekeyed from KFDs. In this case, the partner agencies have implemented a successful encryption management strategy using standardized protocols, effective coordination, and secure transmission of encryption keys.

BEST PRACTICE

Develop key management plans with partner agencies to ensure consistent, coordinated key management and maximize communications interoperability.

1 National Public Safety Telecommunications Council Radio Interoperability Best Practices. Accessed July 9, 2020. http://npstc.org/download.jsp?tableId=37&column=217&id=4033&file=BP_11_Managing_Encryption_for_Interop_Resources_180615.pdf.

Case Study #6: Using the National SLN 1-20 Assignment Plan

A county with a P25 radio system wanted a federal agency to join its network for interoperable encrypted communications. The organizations agreed to have the federal agency subscriber units affiliate with the county KMF for key management and distribution. However, when attempting to program the radios, they found that the county had not coordinated its SLN assignments with NLECC and had already programmed its own agency specific key in the slot designated for the interoperable encryption key. This caused programming conflicts between the two agencies and did not allow them to share encrypted communications. The county had to implement a time and resource intensive network-wide radio reprogramming initiative to correct the issue so that they could have encrypted communications with the federal agency and others in the future.

BEST PRACTICE

Follow the National SLN 1-20 Assignment Plan to avoid programming conflicts and enable encrypted communications among partner agencies.

LMR ENCRYPTION ALGORITHMS

Several encryption algorithms are in use today; however, all encryption algorithms are not equal and do not provide equal levels of security. Two of the most commonly used LMR algorithms, supported by accredited technical standards, are Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

The National Institute of Standards and Technology (NIST) is the federal agency that defines cryptology standards within the Federal Government and is recognized as the country's leading authority on encryption. Its series of publications NIST SP 800-57 outlines requirements for federal agencies regarding key management best practices, policies, and planning, as well as guidance for nonfederal organizations.

NIST strongly recommends the use of AES encryption for public safety communications.

The DES algorithm, developed in 1977, was cracked by the Electronic Frontier Foundation in 1997 in 84 days. It was cracked again in 1998 and twice in 1999, each time in fewer and fewer days.[2] More recently, claims surfaced that the

2 "The Day DES Died." SANS Institute. July 22, 2001. https://www.sans.org/reading-room/whitepapers/vpns/day-des-died-722.

DES algorithm had been cracked in 25 seconds. Faced by the inherent weakness of the DES algorithm, in 2005 NIST withdrew its approval of DES as an encryption standard.

In 1997, NIST announced the new encryption algorithm AES, a more efficient and secure means of encrypting critical information. There is no record of AES ever being cracked, and today NIST encourages federal agencies to use AES for encrypting public safety radios.

Although NIST withdrew its endorsement of DES and DES is no longer supported in the P25 Standards, public safety agencies continue to use it. LMR manufacturers continue to develop products that incorporate DES as well as their own proprietary encryption algorithms. This widespread and inconsistent use of non-AES encryption solutions across the public safety community threatens security and hinders multi-jurisdictional interoperability.

While NIST's jurisdiction is limited to federal telecommunications systems, it has updated its cryptographic standards and key management documents to support private-sector and nonfederal government key management and make them consistent with the Cybersecurity Enhancement Act of 2014. In addition, in order to interoperate with encrypted federal communications systems, nonfederal agencies must adhere to the NIST standards, including the use of AES encryption. These standards have been readily adopted by LMR manufacturers and the user community to ensure common application across multi-vendor platforms and enhance encrypted interoperability.

BEST PRACTICE

Use the AES encryption algorithm and avoid DES and other nonstandard algorithms.

BEST PRACTICES

NIST recommends that "All keys need to be protected against modification, and secret and private keys need to be protected against unauthorized disclosure. Key management provides the foundation for the secure generation, storage, distribution, use, and destruction of keys."[3] The FPIC Encryption Focus Group, in cooperation with NLECC and NIST, have identified the following encryption key management best practices in Table 1.

3 NIST Special Publication 800-57 Part 1 Revision 5. May 4, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf.

Table 1. Encryption Key Management Best Practices

Operation	Best Practices
Purchase multi key radios	■ Purchasing multi key radios provides more flexibility for interoperability, including OTAR ■ Single key radios hamper interoperability and greatly increase programming workload
Obtain keys from the NLECC and follow NLECC recommendations	■ NLECC provides a centralized, secure mechanism for receiving national interoperability keys and unique encryption keys ■ NLECC provides keys only to KFDs with all Wi-Fi capabilities disabled ■ The elimination of static keys can reduce the chances of a key being compromised ■ Agencies must develop procedures to notify NLECC of lost/stolen radios loaded with NLECC keys to enable NLECC to take corrective action ■ Organizations should follow the National SLN Assignment Plan ■ Organizations should work with NLECC to plan their cryptographic strategies and policies
Establish a key management standard operating procedure	■ Define procedures required to report any lost or stolen device within 24 hours; identify procedures for emergency re-key if applicable ■ Establish a key change schedule ■ Identify key management authorities, roles, and responsibilities ■ Communicate and regularly update operating procedures to include surrounding jurisdictions and minimize interoperability issues
Maintain a subscriber unit inventory	■ Document all subscriber units and associated encryption keys so that any vulnerabilities can be removed if a compromised or lost device is discovered ■ If a key is compromised or a device is reported lost, execute a key change or otherwise remove the vulnerability from the system
Maintain the security of encryption key fill devices	■ Develop security protocols to ensure only authorized access to and use of KFDs ■ Consider always using an end-to-end encryption landline to avoid the use of any type of wireless KFD

Operation	Best Practices
Develop an interoperability encryption plan	■ Formalize an encryption policy among all applicable stakeholders ■ Have partner agencies agree to all the key management parameters, including who controls the keys, how the agencies access the keys, when and how the keys are updated ■ Develop communication plans with neighboring jurisdictions to ensure encrypted interoperability ■ Implement MOUs/MOAs where practical to formalize key management and governance processes with partner agencies
Identify key generation method	If not using NLECC for key generation: ■ **Never** manually generate encryption keys ■ Always use a NIST-approved key generation method ■ Refer to Federal Information Processing Standards (FIPS)-approved and NIST-recommended key generation methods available from the Cryptographic Toolkit
Use standardized encryption protocols; sunset use of DES	■ Avoid using DES for encryption as the algorithm is no longer authorized by NIST ■ Use only validated FIPS 140-2 encryption algorithms

NLECC PROCESSES AND PROCEDURES

NLECC generates and distributes national interoperability keys for SLNs 1-20, as well as unique encryption keys for individual agencies' use. It can also provide short-term special operations voice and data encryption keys in situations where limited use keys are needed. NLECC maintains a database of assigned keys to prevent key overlap and conflicts among agencies.

NLECC has established the following voice privacy security settings[4]:

- **Level 1: Clear voice.** No security. Assumes all communications and data transmissions are being monitored.

4 These security settings are established by NLECC for its operations and should not be confused with the security requirements established in NIST's FIPS 140 - 2.

- **Security Level 2: Non-changing (static) secure voice encryption using DES-Output Feedback (OFB) or AES 256 keys.** Initially provides a high level of security but over time, as radios are lost, stolen, or misplaced, the likelihood of compromise increases significantly.[5]
- **Security Level 3: Monthly changing secure voice and data encryption DES-OFB keys.** Provides a high level of voice and data communications security; however, DES-OFB encryption has been compromised and is vulnerable to attack.
- **Security Level 4: Monthly changing AES 256 key secure voice and data encryption keys.** Provides a very high level of voice and data communications security.
- **Security Level 5: One-time, highly restricted and limited-use tactical operations AES 256 secure voice and data encryption keys.** Provide the maximum level of voice and data communications security because the user groups are small, and the crypto period is short.

In most cases, agencies wishing to receive interoperable encryption keys from NLECC must execute an MOU with NLECC that outlines each organization's roles and responsibilities in the key management process. Once the MOU is in place, NLECC will configure and test the agency's KFD(s) to ensure it meets NLECC's key management requirements. Agencies must ensure that proper protocols are in place to securely disseminate the keys only to authorized equipment and protect the keys from unauthorized access. Agencies are required to notify NLECC if any equipment containing encryption keys is lost or stolen so that NLECC can take necessary mitigation steps.

In certain circumstances, NLECC may determine that providing encryption keys to federal, state, and local agencies where no specific MOU for OTAR and key management services exists is in the best interest of CBP.

Organizations can contact NLECC at nlecc-wsoc@cbp.dhs.gov for more information.

5 NLECC recognizes that AES provides stronger security, however, DES keys are still provided in order to support partner agencies that only have DES encryption capabilities. The use of static keys, whether AES or DES, introduces additional risk due to the likelihood of compromise, and therefore are assigned a low security level.

CURRENT GRANT FUNDING REQUIREMENTS RELATED TO ENCRYPTION

Using standards-based encryption is required for certain federal grant funding opportunities. The FY 2020 SAFECOM Guidance on Emergency Communications Grants recommends grant recipients purchase standards-based LMR equipment, including AES 256-bit encryption compliant devices as described in the P25 Block Encryption Protocol.

Agencies planning to use federal grant funding for P25-compliant equipment with encryption must ensure that they implement 256-bit AES encryption. The use of DES encryption algorithms is strongly discouraged. Although P25 standards designate AES as the primary encryption algorithm, it does allow DES-OFB for backwards-compatible interoperability with existing LMR systems.

SAFECOM also strongly recommends that agencies use AES encryption in order to interoperate with federal agencies. Agencies not purchasing AES-encrypted equipment with federal funding must provide written justification for their decision. Additional SAFECOM guidance materials are provided in **Appendix B**.

In addition to P25 standards-based equipment, grant recipients should purchase equipment that that has gone through the P25 Compliance Assessment Program (P25 CAP). This voluntary program enables LMR equipment suppliers to verify their equipment is P25-complaint through testing at a Department of Homeland Security-approved testing laboratory. In the absence of published CAP testing results, agencies are encouraged to identify applicable published interoperability test procedures to validate P25 interoperability compliance. Information on P25 CAP compliant devices can be found on the Approved (Grant-Eligible) Equipment page at https://www.dhs.gov/science-and-technology/approved-grant-eligible-equipment.

For more information on P25 CAP, visit https://www.dhs.gov/science-and-technology/p25-cap.

SUMMARY

Implementing and managing effective encryption involves adopting standards-based technical and management policies. The most fundamental best practices are:

- Before making encryption decisions, consult with other agencies who have encryption experience or encryption-focused organizations;
- AES 256 is a standard encryption algorithm that provides adequate security without impeding interoperability;
- Coordinate your encryption strategy ahead of time with your SWIC and mutual aid agencies;
- Purchase radios with multi-key encryption capability and follow the National SLN Assignment Plan when assigning key slots; and
- Design a key management plan that maintains equipment and encryption keys securely and includes policies regarding lost or stolen radios, key distribution, records of assets, and regular rekeying of all radios.

For any further questions or assistance, contact the FPIC at FPIC@cisa.dhs.gov or any of the contacts listed in **Appendix A**.

APPENDIX A: POINTS OF CONTACT

For additional information regarding the implementation and management of P25 land mobile radio encryption systems, the following points of contact are provided:

- The National Law Enforcement Communications Center (NLECC): nlecc-wsoc@cbp.dhs.gov
- Statewide Interoperability Coordinator (SWIC) for each of the 56 states and territories: www.cisa.gov/safecom/ncswic-membership
- The Federal Partnership for Interoperable Communications (FPIC) Security Working Group: FPIC@cisa.dhs.gov

APPENDIX B: DOCUMENTS

FPIC Encryption Trio
- *Guidelines for Encryption in Land Mobile Radio Systems*
- *Considerations for Encryption in Land Mobile Radio Systems*
- *Best Practices for Encryption in P25 Land Mobile Radio Systems*

https://www.cisa.gov/publication/encryption

Security Requirements for Cryptographic Modules (FIPS PUB 140-2)
https://csrc.nist.gov/publications/detail/fips/140/2/final

NIST Withdraws Outdated Data Encryption Standard
www.nist.gov/news-events/news/2005/06/nist-withdraws-outdated-data-encryption-standard

NIST Key Management Guidelines
https://csrc.nist.gov/Projects/Key-Management/Key-Management-Guidelines

NIST Special Publication 800-53 Revision 4
Security and Privacy Controls for Federal Information Systems and Organizations
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST Special Publication 800-57 Part 1 Revision 5,
Recommendation for Key Management Part 1: General
https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

NIST Special Publication SP 800-57 Part 2 Rev. 1
Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations
https://csrc.nist.gov/publications/detail/sp/800-57-part-2/rev-1/final

NIST Special Publication SP 800-57 Part 3 Rev. 1
Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance
https://csrc.nist.gov/publications/detail/sp/800-57-part-3/rev-1/final

NIST Special Publication 800-130
A Framework for Designing Cryptographic Key Management Systems
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf

NIST Special Publication 800-131A Revision 2
Transitioning the Use of Cryptographic Algorithms and Key Lengths
https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final

NIST Special Publication 800-175A
Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies
https://csrc.nist.gov/publications/detail/sp/800-175a/final

NIST Special Publication 800-175B Rev. 1
Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
https://csrc.nist.gov/publications/detail/sp/800-175b/rev-1/final

Federal Information Security Modernization Act of 2014
https://www.cisa.gov/federal-information-security-modernization-act

The E-Government Act of 2002 (FISMA public law 107-347)
https://www.govinfo.gov/app/details/PLAW-107publ347

Fiscal Year 2020 SAFECOM Guidance on Emergency Communications Grants
https://www.cisa.gov/publication/funding-documents

APPENDIX C: RECOMMENDED NATIONAL RESERVED SLN TABLE

Recommended National Reserved SLN Table

SLN	Algorithm	Use	SLN Name	Crypto Period	Authorized Users
1	DES	Public Safety Interoperable	ALL IO D	Annual	All Network Users
2	DES	Federal Interoperable	FED IO D	Annual	All Federal Network Users
3	AES	Public Safety Interoperable	ALL IO A	Annual	All Network Users
4	AES	Federal Interoperable	FED IO A	Annual	All Federal Network Users
5	DES	National Law Enforcement State and Local Interoperable DES	NLE IO D	Static	All Federal, State, and Local Law Enforcement
6	AES	National Law Enforcement State and Local Interoperable AES	NLE IO A	Static	All Federal, State, and Local Law Enforcement
7	AES	US – Canadian Federal Law Enforcement Interoperability	FED CAN	Static	All US - Canadian Federal Law Enforcement
8	AES	US – Canadian Public Safety Interoperability	USCAN PS	Static	All US and Canadian Public Safety Users

SLN	Algorithm	Use	SLN Name	Crypto Period	Authorized Users
9	DES	National Tactical Event	NTAC D	Single Event Use – Not to exceed 30 Days	All Federal, State, and Local Public Safety
10	AES	National Tactical Event	NTAC A	Single Event Use – Not to exceed 30 Days	All Federal, State, and Local Public Safety
11	DES	Multiple Public Safety Disciplines	PS IO D	Static	All Federal, State, and Local Public Safety
12	AES	Multiple Public Safety Disciplines	PS IO A	Static	All Federal, State, and Local Public Safety
13	DES	National Fire/EMS/Rescue	NFER D	Static	All Fire/EMS/ Rescue Users
14	AES	National Fire/EMS/Rescue	NFER A	Static	All Fire/EMS/ Rescue Users
15	DES	National Task Force Operations	FED TF D	One time use as needed for Special OPS	Federal Task Force
16	AES	National Task Force Operations	FED TF A	One time use as needed for Special OPS	Federal Task Force
17	DES	National Law Enforcement Task Force (one time only operation)	NLE TF D	One time use as needed for Special OPS	All Federal, State, and Local Law Enforcement

SLN	Algorithm	Use	SLN Name	Crypto Period	Authorized Users
18	AES	National Law Enforcement Task Force (one time only operation)	NLE TF A	One time use as needed for Special OPS	All Federal, State, and Local Law Enforcement
19	AES	Federal – International Law Enforcement Interoperability	FED INTL	When needed by operational requirement	Federal and Visiting International Law Enforcement
20	AES	Public Safety – International Law Enforcement Interoperability	PS INTL	When needed by operational requirement	All US and Visiting International Public Safety

APPENDIX D: FPIC ENCRYPTION TRIO FACT SHEETS

Considerations for Encryption in Public Safety Radio Systems

Determining the Need for Encryption in Public Safety Radios

We live in an ever-changing world, and the world is becoming a more complicated and dangerous place to live and work. This heightened danger has caused public safety agencies to place greater importance on how they use technology and how they enhance their ability to protect and serve. Since the terrorist attacks of September 11, 2001, public safety continues to rethink communications strategies to meet new challenges. Today many public safety communications channels get streamed across the Internet and are openly broadcast to the public, media, criminals, and potential terrorists providing immediate access to sensitive public safety information.

As agencies work to enhance interoperability, they also have to remain keenly aware of the need to protect sensitive public safety communications. Compromised information can be used to hinder emergency response, impede investigations and surveillance, or endanger the public. Many public safety agencies combine local, regional, or statewide government communications needs into multi-jurisdictional or multi-discipline systems. These large shared systems often integrate public safety, public service, maintenance, and administration into a single radio system. Although all of these disciplines are not always critical to the safety of life, they *do* support law enforcement, firefighting, and emergency medical missions that include:

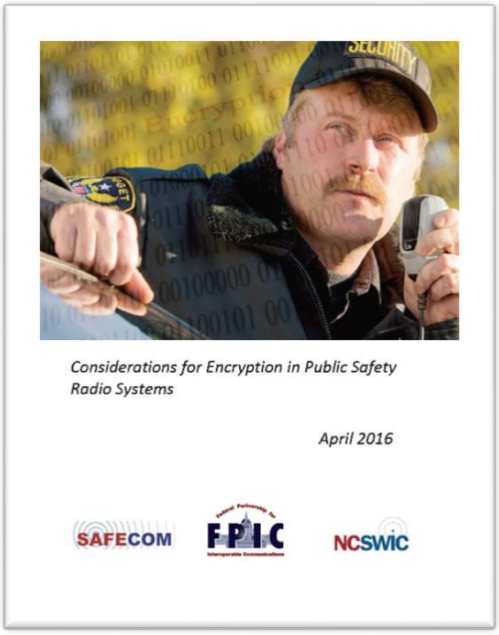
- **Safety of personnel, and enhanced safety of the public and property**
- **Sensitive law enforcement information including active investigations and surveillance**
- **Personally identifiable information or protected health information**
- **Tactical/investigative information that may jeopardize law enforcement operations, and**
- **Disaster incident information that may reduce reaction abilities of public safety officials**

In many cases, public safety radio communications are transmitted "in the clear[1]," removing protection from monitoring by someone with a basic knowledge of radio communications by using fairly simple over the counter equipment. In a threat-based environment, compromise of any information can be problematic and may jeopardize safety and mission integrity. Radio encryption would help to decrease a threat of compromise and reduce the risk to personnel safety while providing protection of sensitive information.

[1] "In the clear" transmissions are unencrypted radio signals that are open to reception and listening by anyone with a receiver.

THE REPORT

This document examines why encryption may be necessary during critical operations. Encryption provides a method of protecting personally identifiable and/or sensitive information. Different jurisdictions may have differing legal requirements relating to encryption of communications on public safety radio systems. Therefore, when considering encryption, a legal analysis should be conducted. Recent incidents illustrate why encryption is a must for public safety are discussed in this document. They include:



- **Active shooter**
- **Public knowledge of sensitive public safety information**
- **Safety of public safety personnel and the public**

Other scenarios might involve Urban Search and Rescue, training, emergency response, active investigation and surveillance, personally identifiable information, and scanners/social media are discussed. The examples discussed in the document provide examples of how encryption did or would have affected the outcome of public safety actions regarding criminal activity or the compromise of protected personal information.

IMPLICATIONS FOR THE PUBLIC SAFETY COMMUNITY

Radio encryption provides the best way to protect critical information from compromise and disclosure when necessary to transmit it over the airways. Use of encryption is an important policy decision that stakeholders, decision-makers, and leadership must understand and carefully consider as they plan for the future. Encryption can significantly decrease the risk that sensitive public safety information can be compromised and used to impede effective emergency response. The policy and legal decision to encrypt is not without complexities. The threat of compromise of critical information resulting in increased threats to the safety of the public is clear.

Before decision makers decide when and how to encrypt, it is important to consider what information to protect. Each jurisdiction will have differing perspectives; the primary questions to be addressed will include:

- **What information should be protected (encrypted)?**
- **What method of encryption should be implemented?**
- **What is the impact on communications interoperability?**
- **What about the added cost vs. the impact of compromise?**
- **What is the effect on public information access?**

All the factors discussed in this document should be carefully considered in determining the appropriate encryption for that public safety radio system in that specific jurisdiction. Federal agencies recognize the importance of encrypting public safety mission critical radio communications and embrace the fact that encryption is vital to national security and mission integrity. State and local governments must answer for themselves the basic question: *Does the cost and effort related to the implementation and management of encryption outweigh the risks associated with the exposure of sensitive information?*

This document is provided to guide public safety users through a process to assess the need for encryption as well as the questions that must be considered.

Guidelines for Encryption in Land Mobile Radio Systems

Determining what Encryption Method to use for Public Safety Radios

As a result of a growing number of incidents involving the vulnerability and subsequent compromise of sensitive information, the public safety community recognizes the importance of protecting information transmitted over its wireless communications systems. The implementation of digital land mobile radio (LMR) technology, such as Project 25, increases the awareness that encryption provides required protection more readily than was available for analog systems.

The key to protecting sensitive operational or safety of life radio transmissions is to deploy an encryption system with an algorithm that assures information is adequately protected from eavesdropping. A number of encryption algorithms exists that employ encryption key lengths from 56 bits to 256 bits. These techniques are used in LMR systems throughout the United States and the world, but not all provide the protection needed to guarantee information security.

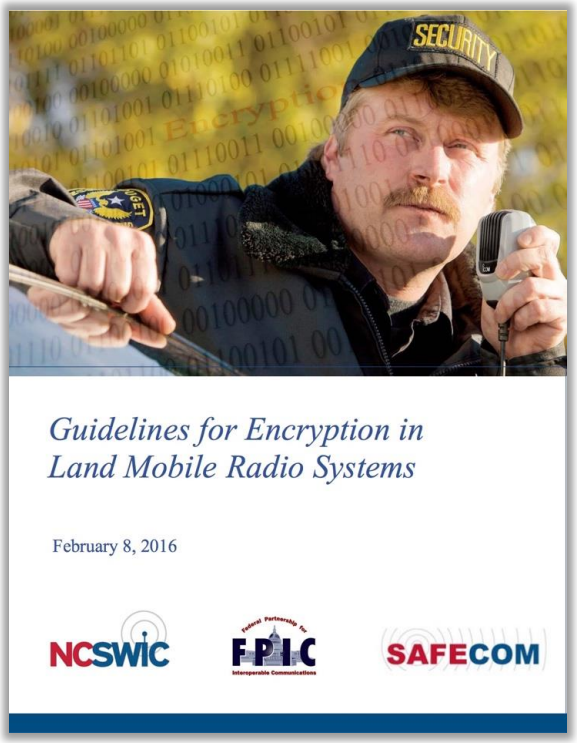
Standards-compliant algorithms, such as the Advanced Encryption Standard (AES), offer the greatest opportunity for achieving maximum interoperability while providing a high level of information security. The AES algorithm is specified in the National Institute of Standards and Technology (NIST) FIPS PUB-197[1]. Unlike proprietary or non-standard algorithms, AES is freely available to any manufacturer who wishes to use it. There are no intellectual property restrictions or royalty payments involved with its use. While key lengths of 128-bit and 192-bit are authorized for use, it is strongly recommended that the 256-bit key is utilized in public safety wireless systems in accordance with the published standard for Project 25 Block Encryption Protocol (TIA-102.AAAD-B).

THE REPORT

Most public safety system administrators and managers want to minimize the possibility of sensitive information being monitored by the use of low-cost scanners or other devices and are concerned with the added complexity and cost of standards-compliant encryption. Other documents, in a series of encryption-related reports published by SAFECOM/NCSWIC/FPIC, will outline these issues. The goal of this document is to provide information that should be considered when evaluating encryption solutions, especially what encryption techniques to consider and those to avoid.

[1] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

The primary objective of this document is to discuss methods that may be used to ensure the privacy of sensitive public safety LMR communications. These methods mainly involve the use of a variety of encryption techniques. The report outlines what encryption algorithms are considered safe or "cryptographically strong" enough to be highly resistant to unauthorized decryption. For the protection of sensitive public safety information, the "strongest" algorithm available for LMR systems today is AES, with a 256-bit key length. In general, the "strength" of an algorithm directly corresponds to its key length, or the number of possible keys… the greater the number of keys, the less likely the key can be determined by an adversary.



IMPLICATIONS FOR THE PUBLIC SAFETY COMMUNITY

Encryption provides the best way to protect critical information from compromise and disclosure, it can also complicate the implementation of interoperable land mobile radio systems. In order to be interoperable in an encrypted environment, LMR systems must use the same type of encryption and share the same key management parameters. Those that use non-standard encryption algorithms or techniques will not interoperate with systems that use P25 Standard encryption. Although DES and AES are P25 Standards compliant, they will not interoperate, so consideration should be given to which technique to implement.

SAFECOM, NCSWIC, and FPIC recommend that AES-256 encryption is the goal for all public safety agencies to ensure the greatest protection against potential compromise of sensitive information and the best chance to improve encrypted interoperability. The DHS Office of Emergency Communications, in its National Emergency Communications Plan (NECP) of 2008, detailed an initiative to "… *implement the Advanced Encryption Standard (AES) for Federal responders. A standard nationwide encryption method will diminish the interoperability challenges faced by Federal responders (who previously used different methods) and will provide guidance to local and State agencies when working with Federal agencies"* and…to establish "*AES as the uniform standard for State, local, and tribal emergency responders who decide to use encryption*". Although the NECP has since been updated, the soundness of the initiative remains valid today and extends to all public safety agencies. Simply put, encryption for the Nation's first responder communications systems assures the protection of sensitive information from unauthorized use.

This Fact Sheet is a brief summary of the SAFECOM/NCSWIC/FPIC encryption document entitled *Guidelines for Encryption in Land Mobile Radio Systems*, published on the DHS Technology Website at http://dhs.gov/Technology under "Encryption".

Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems

Developing Methods to Improve Encrypted Interoperability in Public Safety Communications

The encryption of public safety land mobile radio systems is a decision that many public safety agencies are contemplating or have made in recent years. It is a primary method of mitigating threats from the potential compromise of personal or sensitive data and can enhance operational security as well as improve interoperability. Protecting land mobile radio systems and the information they transmit from unauthorized interception and use is increasingly important to maintaining effective public safety communication and response.

Successful encrypted interoperability depends largely upon improved coordination between agencies needing to interoperate. Encryption key management is also enhanced when all agencies understand how to use and coordinate key management. Improperly managed key parameters can affect radio users' ability to interoperate. If agencies choose to implement encryption, it is important that encryption and key management becomes an organizational priority implemented in a consistent manner across all public safety agencies with interoperability needs.

THE REPORT

The Federal Partnership for Interoperable Communications (FPIC), in coordination SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC), developed this report in response to a growing need to improve encrypted interoperability at all levels of government. The *Best Practices* discussed in this document provide an overview of how basic key management parameters are related in Project 25 land mobile radio (P25 LMR)[1] systems. The document also addresses methods to improve cross-agency coordination, and emphasizes the use of standards-based encryption, to enhance secure interoperability minimizing the risk of compromising sensitive information. Primary *Best Practices* to improve encrypted interoperability include:

- **Key Management Organization** – Develop an effective key management structure.
- **Key Generation and Distribution** – Adopt P25 standard key parameters for enhanced interoperability.
- **National SLN Assignment Plan** – Adopt a standardized Storage Location Number (SLN) plan to minimize conflicts.

[1] Project 25 was previously referred to as APCO Project 25, now simply P25.

- **Standards-based Encryption** – Use P25 standard AES-256[2] security solution to protect against compromise.
- **Crypto Period Considerations** – Define and implement feasible crypto periods to mitigate risk.
- **Communications Planning** – Develop Communications Plans that incorporate encryption requirements.
- **Education and Training** – Develop appropriate training for both system personnel and field operational users to improve effectiveness.
- **Exercise and Testing** - Develop and execute regular communications exercises and testing to maintain effectiveness.
- **Outreach** – Collaborate with knowledgeable experts to ensure effective encryption implementation.

This document also highlights best practices of key management necessary to allow encrypted operability and interoperability. Fundamentally, the intent of this document is to simplify the complex process of encryption and key management and discuss *the essential elements or parameters that are needed for operability and interoperability*. This document identifies *Best Practices* for basic aspects of key management, making encrypted interoperability is possible and manageable among public safety agencies at all levels of government.

ANSI/TIA 102 Series of Project 25 Standards explain how encryption works in a P25 system and how encryption protects sensitive information. The National Institute of Standards and Technology (NIST) SP 800-57 series of publications describe methods of key management. This document provides details on how and why specific encryption parameters are crucial to maintaining system security and enable interoperability in the encrypted mode.

IMPLICATIONS FOR THE PUBLIC SAFETY COMMUNITY

These best practices are important in developing security where encrypted interoperability is realizable. Additionally, significant planning and coordination must be undertaken to achieve encrypted interoperability on a national scale. Leadership in developing more detailed encryption guidelines and further education of the user community must occur. These best practices align with the guiding principles of the Interoperability Continuum.[4] The goals are based on increased interoperability by effective leadership, planning, and collaboration among public safety agencies. To that end, adherence to established *Best Practices* for encryption will provide

- **Cost efficient implementation**
- **Effective protection of sensitive information**
- **Credible standards-based policy development**
- **Successful encrypted interoperability during multi-agency emergency response**

The public safety community can achieve encrypted interoperability at the local, regional, state, and national level by collaborating with the other users and encryption experts. Effective planning, cooperation, governance, and a basic understanding of how key parameters are coordinated can lead to successful *Encrypted Interoperability*.

[2] NIST FIPS 197, *Advanced Encryption Standard*, Nov 2001
[3] NIST SP-800-57, *Recommendation for Key Management, Parts 1-3*
[4] https://www.cisa.gov/publication/commonly-accessed-documents-safecom