The Who, What, When, Where, How, and Why of Encryption in P25 Public Safety Land Mobile Radio Systems

Publication: 2023
Cybersecurity and Infrastructure Security Agency

How to Use This Document

Overview of Document Navigation Features

This document incorporates navigability features which allow the reader to easily "click" and transition to specific focus areas and subsections of the document. The navigation "click" feature is incorporated in two locations; the document's Table of Contents and a Bookmark Icon Bar, located at the top of each page of the document (starting at page 9).

These clickable features are intended to allow readers to easily navigate to the section of their choosing within the document. However, reading the document in its entirety is encouraged.

Navigation to Focus Areas and Subsections via the Table of Contents

The document is organized into four focus areas, which include:

1. **Considering Encryption: The Need and the Issues**
2. **Guidelines for Making Good Technology Choices**
3. **Best Practices for Encryption Key Management**
4. **Appendices**

These focus areas are highlighted with specific colors and are accompanied by their representative subsections. The subsections provide the relevant information and in-depth content regarding the highlighted focus areas. Each focus area and their subsection within the Table of Contents is clickable, allowing direct movement to any focus area or subsection within the document.

Navigation to Focus Areas via the Icon Bookmark Bar

In addition to the "click" navigation feature provided in the **Table of Contents**, an Icon Bookmark Bar is provided at the top of each page (starting at page 9), allowing navigation to any of the four focus areas of the document.

To navigate to specific focus areas, simply "click" on the focus area icon of your choosing, and it will automatically take you to the page where the selected focus area begins.

Table of Contents

List of Figures

Preface

Wireless communication is the backbone of public safety operations. Public safety responders' ability to talk with one another and coordinate efforts during routine operations, planned events, and emergency responses is a key factor in saving lives and protecting property. Reliable communications via land mobile radio (LMR) depends on many elements—technology, interoperability, preparation, and training. In recent years, another element has gained importance: security. So much so that encryption has become a primary focus of the public safety community.

Much emphasis on encryption arises from public concern over privacy and the duty of public safety entities to provide such privacy while also protecting sensitive information. No one wants their personal health information (PHI) or personal identifiable information (PII) broadcast over an open radio channel. Public safety officials have their own security concerns. With the proliferation and online availability of radio scanners, scanner applications, frequency jammers, and radio cloning devices, how can officials protect wirelessly transmitted information about investigations and tactical operations? In the aftermath of a crime, how do officers keep operational information confidential when setting up roadblocks or establishing search areas? During a disaster, how do rescue teams share critical information free from eavesdropping, which could lead to news coverage or crowds that may disrupt a life-saving operation?

The best available solution is encryption. Also referred to as *cryptography*, encryption is a technology that encodes voice and data traffic in such a way that only recipients with appropriate equipment can decode. It is an effective method for protecting sensitive communications, and many agencies have established robust encryption plans, while others are evaluating and expanding their encryption usage. While encryption is crucial for security, its use must not hinder the operation or capabilities of an agency's communications system nor its interoperability with surrounding jurisdictions and mutual aid partners.

This guide provides readers new to the topic of encryption with a discussion of basic issues related to establishing and maintaining effective encryption for Project 25 (P25) interoperable LMR communications systems. It combines and updates the content of three previously published documents issued by the Federal Partnership for Interoperable Communications (FPIC), SAFECOM, and the National Council of Statewide Interoperability Coordinators (NCSWIC) in 2016; namely:

- *Considerations for Encryption in Public Safety Radio Systems*: This document examines why encryption is necessary during critical operations. The document provides examples of how encryption decreases the threat of compromise and reduces the risk to personnel safety while providing protection of sensitive information.

- *Guidelines for Encryption in Land Mobile Radio Systems:* This document provides information that should be considered when evaluating encryption solutions to protect sensitive operational or life safety radio transmissions.
- *Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems:* This document discusses encryption best practices for P25 LMR systems. The document also provides an understanding of how basic key management parameters are related in P25 LMR systems.

The document adds to the previous publications an extensive new section on encryption key management, based on current proven encryption practices.

The overall objective is to further define and explain encryption and provide reliable guidance for planning, implementing, and managing an LMR encryption strategy. Special emphasis is on two core issues: 1) establishing common procedures—including governance, policies, and training—to preserve user-defined interoperability and 2) managing encryption keys, the random strings of bits used to encode and decode data.

Be aware that federal departments and agencies must adhere to security requirements beyond those presented here, according to Congressional legislation, regulations, and policies. These requirements are more stringent than those required for most state, local, tribal, and territorial entities. In addition to following the guidance in this document, public safety practitioners and their agencies should be aware of such regulations and policies affecting federal and other agencies with whom they interoperate. Adhering to those same policies not only makes interoperability more efficient but can also enhance state, local and tribal security, help ensure the privacy of citizens, and better position agencies for future federal grant programs related to communications.

This document will not address all questions. It should give agencies a basic understanding of encryption and the importance of the role of encryption in wireless information security. The document also provides guidelines to consider the level of encryption requirements, specifically when using P25 LMR systems. Finally, this document describes how to properly implement encryption on a P25 LMR system. It also offers the benefit of having been crafted by practitioners with many years of experience from across the country, who, often after much trial and error, have successfully implemented robust encryption capabilities in their jurisdictions.

For more information on encryption, and for answers to specific questions about encryption, please contact the FPIC at FPIC@cisa.dhs.gov

Acknowledgments

This report is the result of many months of intensive effort by the FPIC and scores of local, state, tribal and federal partners. We would like to thank all those partners involved in the development of this document. Specifically, we would like to thank those engaged with FPIC's Security Subcommittee, who helped generate support, provided subject matter expertise, and devoted their time to this endeavor.

Considering Encryption: The Need and the Issues

The implementation and use of encryption for wireless communications for federal agencies was implemented by President Ronald Reagan in 1984, with the passing of the National Security Decision Directive (NSDD) 145. This directive was then expanded in 1987 to cover all non-government computer systems. While federal agencies are mandated to follow this directive, encryption for non-federal agencies is not mandatory under this directive. However, non-federal agencies should seriously consider the implementation and use of encryption due to the following factors:

- increasingly serious criminal attacks and breaches of wirelessly transmitted information among the general public and within the public safety community
- occurrences of social unrest which have exposed vulnerabilities of law enforcement channels
- escalating frequency of confidential and sensitive transmissions within public safety communications
- availability of commercial off-the-shelf scanning and eavesdropping technologies

Experienced practitioners recognize that encryption is the best means to protect critical information transmitted over the air. They also realize the importance of reliable interoperability among agencies' radio systems at all levels. Many believe that implementing encryption decreases efficient interoperability. However, when properly planned, designed, implemented, and maintained through methodologies and governance policies, efficient and effective encrypted interoperability can be achieved.

Many agencies have proven that both efficient wireless security and interoperability are achievable.

What is Encryption?

Digital radio encryption is the process of using an algorithm (set of computer instructions) to encode wireless information (voice or data) in such a way that it is unintelligible to anyone without the hardware or software needed for decoding and decryption. In the transmitting radio, the algorithm uses a unique string of random bits (an encryption key) to encode the information. To decode it, the receiving radio must be equipped with an identical encryption key. Anyone might be able to intercept an encrypted transmission, but only someone with the appropriate encryption key can decode the information into an intelligible form.

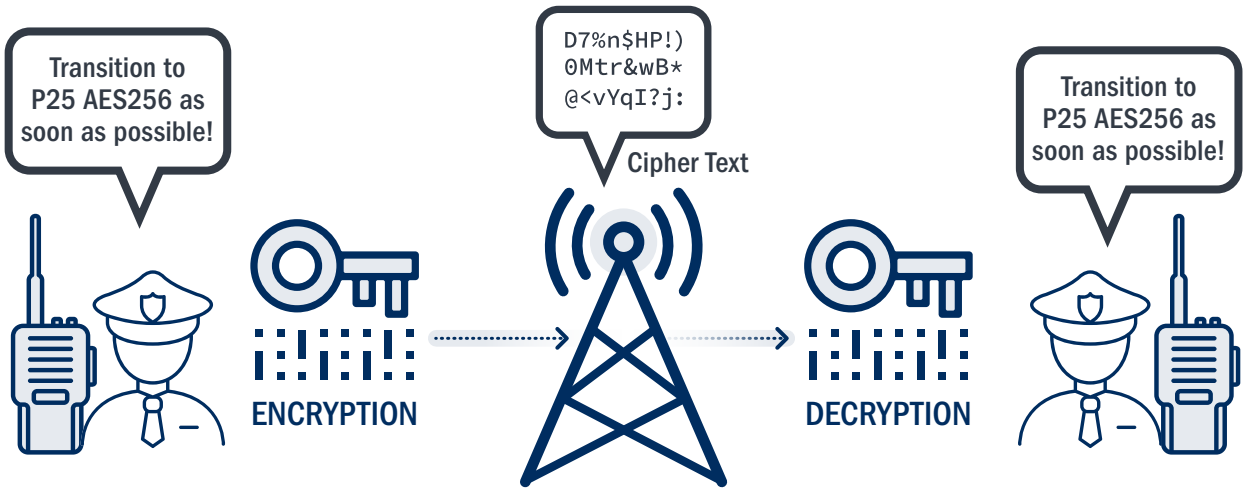


Figure 1. Digital radio encryption process

As simple as the concept is, establishing and maintaining a comprehensive encryption plan that provides adequate security without hampering interoperability can be a steep governance and technical challenge. Yet scores of agencies and their mutual aid partners across the country have resolved this challenge. Their experience is the foundation of the information provided in this document.

Why Should You Encrypt?

The best rationale for encryption lies in the potential ramifications of not encrypting critical radio communications. Many public safety incidents illustrate the impact of open (non-encrypted) radio communications, especially in law enforcement. Among them:

- During recent civil protests, law enforcement personnel were called to control rioting in a downtown section of a major city. Protesters using smartphone-supported scanner applications monitored law enforcement channels and informed the crowds about police locations and activities, facilitating looting, arson, and assaults on responding law enforcement personnel.
- Along the Southwest border and in other jurisdictions around the country, technologically sophisticated criminals routinely sift through law enforcement transmissions to gather information on tactical operations and locations of law enforcement units, as well as citizen PII—driver license numbers, birth dates, etc.—jeopardizing officer safety and operations and putting citizens at risk of identity theft.
- During a recent Super Bowl, a copy of the public safety units' communications plan leaked to the public domain. A local hacker created a web-based listing of all the radio channels, the intended channel usage, and assigned users. The hacker also listed links to scanner apps

that would permit anyone with a smartphone, laptop, or tablet to scan and listen to any of the unencrypted talk groups/channels.

- In a Southwestern state, law enforcement officers responding to an active shooter incident across several locations quickly developed information from the crime scenes that lead to suspects' identities and potential new targets. When the suspects' location was confirmed, investigators broadcasted the information over an unencrypted dispatch channel to patrol officers and tactical teams. Media outlets listening to the channel set up a live broadcast at the suspects' location before law enforcement teams arrived. The situation posed a significant safety issue for the media crews and, by eliminating the element of surprise, put the officers at risk and compromised their tactical plan. Combined with similar leaks of information about juvenile suspects, fugitives, criminal investigations, and surveillance and tactical operations, the incident convinced the police department to encrypt a larger portion of their radio traffic.
- Police in a Southeastern state were stymied by a rash of home invasions and robberies targeting one ethnic group. They determined the perpetrators were using radio scanners to monitor police movements and avoid responding units. County communications officers deployed encrypted radios to the teams detailed to the investigation, and within several days they apprehended the subjects.

The ready availability of radio scanners and scanning apps enable almost anyone to eavesdrop on public safety operations, gather sensitive information, and disseminate it virtually everywhere. One does not have to search extensively on the Internet to find transcriptions and rebroadcasts of federal, state, and local public safety radio traffic. Among the published examples in the National Capital Region, which encompasses Washington, D.C., and surrounding jurisdictions, are United States (U.S.) Department of Homeland Security (DHS) countersurveillance missions, the Federal Bureau of Investigation (FBI) airborne missions, movements of the President of the United States, and surveillance information related to a presidential inauguration.

The lack of active encrypted radio communications can severely impact operations and personnel safety in many situations, for example:

- **Active Shooter Incidents.** Law enforcement response has evolved rapidly to meet the changing tactics of active shooters, and after-action reports regularly highlight the effectiveness of close coordination among responding agencies. Radio systems that enable this coordination give responders a decided advantage over their adversaries, but that advantage is lost when adversaries can monitor police radio traffic using smart phone apps or inexpensive scanners. The use of encryption was an effective solution when implemented.
- **Urban Search and Rescue Team (USART) Deployments.** USART personnel from the Federal Emergency Management Agency (FEMA) and other federal, state, local, tribal, and territorial agencies use encrypted radio systems for simplex, repeated, and trunked talk-groups. However, during disasters such as hurricanes, floods, and wildfires, these teams must

manage, direct and coordinate with other federal, state, local, tribal, territorial agencies who use disparate encryption technologies or none at all. This often forces FEMA and its partners to compromise their encryption strategies to achieve interoperability.

- **Training Exercises.** The best training replicates as closely as possible the types of situations responders might face and requires them to practice procedures they would employ in real incidents. In reported cases, law enforcement training exercises conducted over unencrypted radio channels have exposed confidential surveillance and tactical methods, compromising law enforcement's ability to apprehend criminals and respond effectively to critical situations.
- **Emergency Response.** Unencrypted emergency radio communications give the public and the media unrestricted access to real-time information about incidents ranging from vehicle accidents and structure fires to hazmat spills and in-progress criminal activity. This information often attracts crowds and media units to active response scenes, complicating efforts to control the situation and requiring additional resources, hindering access to emergency vehicles and personnel, and potentially putting the observers in harm's way.
- **Active Investigations and Surveillance.** Investigations and surveillance activities, whether aimed at solving or preventing crimes, rely on stealth and confidentiality. Unencrypted radio communications among stakeout teams and transmissions from body wires to surveillance vehicles are two examples of what can be intercepted by anyone with a scanner. The same holds for fire investigations, where investigators might exchange sensitive information and confidential investigation techniques by radio.
- **Personally Identifiable Information (PII).** PII is any information that identifies a particular individual (e.g., full name, social security number, address, driver's license number, medical insurance number). If unencrypted, this information may be intercepted during traffic stops, routine investigations, or emergencies, and can put citizens at risk of identity theft, identification in the press, or simply embarrassment. Compromising an individual's PII may expose agencies to legal liability.
- **Medical Emergencies.** In addition to attracting crowds and the media to the scenes of medical emergencies, unencrypted emergency medical service (EMS) radio traffic between an ambulance and a treatment facility, a dispatcher, law enforcement, or fire personnel can easily compromise protected health information (PHI) by revealing facts about medical conditions, sexual assaults, domestic abuse, and child endangerment.

  Complicating EMS encryption is the fact that EMS units must be able to communicate with each other, with fire and police units, and with local medical facilities. In addition, some jurisdictions use private or contract-operated EMS/ambulance services, complicating encryption key management and overall communications security.

What Should You Encrypt?

Federal agencies are required by law/policy to use encrypted communications at all times. State, local, tribal and territorial public safety agencies are strongly encouraged to also adopt advanced encryption standard (AES) encryption. All agencies must first identify what information it needs to protect. Agencies should review their jurisdictional legal requirements, operational environment, standard operating procedures, and communication vulnerabilities. This review will provide a sound basis for encryption decisions.

The primary consideration for determining which voice and data transmissions require encryption is the safety of personnel, the public, and property. In this regard, primary candidates for encryption are:

- Sensitive law enforcement information, especially information related to active investigations and surveillance
- PII and PHI of personnel and citizens
- Tactical information that, if released, could jeopardize law enforcement operations
- Disaster incident information that public safety officials rely on to respond quickly and effectively in emergencies

Many agencies combine local, regional, and statewide government communications into multi-jurisdictional or multi-disciplinary LMR or wireless data systems. This often means integrating public safety, public service, maintenance, and administrative functions into a single radio system. Although many of these functions only indirectly affect public safety, they all support law enforcement, firefighting, and emergency medical missions. The information they transmit either routinely or in critical situations should be carefully reviewed to determine what is sensitive enough to require encryption.

Encryption can apply to so many parts of a communications ecosystem that an agency's first impulse might be "let's encrypt everything," but in practical terms blanket encryption can work against an agency. If an agency follows the best practice of using the National Law Enforcement Communications Center (NLECC)[1]—part of DHS Customs and Border Protection (CBP)—to provide its nationwide or regional interoperability encryption keys and coordinates encryption policies with other jurisdictions and mutual aid partners, blanket encryption should not interfere with interoperability. However, if an agency chooses to generate its own encryption keys and fails to coordinate with neighbors and partners, interoperability can be compromised, preventing disciplines from coordinating their efforts.

[1] For a detailed description of NLECC and its functions, see **NLECC: The Role of National Standards and Organization**.

There are also concerns surrounding the implementation of blanket encryption, including lack of transparency to the public and overall cost. Small agencies with limited resources have to be efficient and strategic when implementing, managing, and maintaining an encryption system. Therefore, it is necessary for each agency to identify the most optimal route towards implementing encryption and making sure that they own the process.

Blanket encryption also can raise public complaints about "lack of transparency." And for small agencies with limited resources, cost can be a factor. Implementing, managing, and maintaining an encryption strategy can be costly; extending it to all the information and all the radios and radio systems in an agency multiplies the expense.

How Might Encryption Impact Operations and Interoperability?

Once an agency identifies what information needs encryption, some basic technical questions must be answered:

- Which encryption technologies best meet our security requirements?
- How might those technologies impact communications operations and interoperability?
- What effect would encryption have on the public's legitimate access to information?
- What is the most effective encryption management strategy that fits the agency's budget and resources? AES is essential for security; however, optional functions and features, such as Over-the-Air Rekeying (OTAR), which enables encryption keys in subscriber units to be replaced without physically attaching each unit to a rekeying device, can significantly increase initial capital cost but may prove cost effective over time. For less sensitive communications, employing transmission delays to public broadcast of select channels/talkgroups may be an option.
- Does your agency have appropriate training and processes in place to properly manage the encryption technologies? An effective and repeatable training process with established policies regarding the use and operation of encryption is a must to establish an effective and workable encryption program.
- Periodic assessment of user's proficiency and understanding of encryption capabilities strengthen an effective encryption program.

How LMR Encryption Works: An Overview

Sophisticated encryption requires a digital radio system. Consoles and subscriber units must be encryption-capable, meaning they must have one or more software "slots" for storage of encryption keys. These slots are referred to as Storage Location Numbers (SLN). Radios supporting multiple SLNs are strongly recommended to those radios supporting only single SLNs or single key radios

that can store only one encryption key at a time. Radios supporting multiple slots or multi-key enables users access to encryption keys shared to the radio from different LMR system to support encrypted communications on different channels/talkgroups. This capability helps ensure secure interoperability during cross-disciplinary and multi-jurisdictional operations. Also, OTAR is possible only with multi-key subscriber equipment, so agencies should consider developing a plan, in coordination with other agencies, on how the key management facility (KMF) is going to integrate with other KMFs in the area to share or interconnect.

NLECC and the Federal Partnership for Interoperable Communications (FPIC) created the National Storage Location Numbers Assignment Plan, a common configuration for all public safety P25 LMRs. The plan reserves SLN 1-20 for use for national interoperability. Agencies are strongly advised to follow the national plan and not assign any of their agency keys, contiguous agency keys, regional keys, or state keys to these slots. More information on **The National Storage Location Numbers Plan Table** is on page 38.

The foundation of any encryption strategy is its cryptographic algorithm, the computer instructions that apply the encryption keys to encode and decode voice and data traffic. The algorithm normally is deployed as part of every subscriber unit and dispatch console in an LMR system. AES256 is the only algorithm that complies with the P25 standards and its use is strongly recommended. The section **AES: A Built-In Advantage of Project 25** discusses AES256 in more detail.

In an encryption system, the algorithm that generates keys does not routinely change; however, encryption keys are changed as necessary to preserve the integrity and security of the system.

Radio system owners/operators can choose to generate their own unique encryption keys using the National Institute of Standards and Technology (NIST) recommended Key Generation Methods, defined in NIST SP800 series publications, and a key management facility (KMF), a device for securely managing widely distributed encryption keys. The FPIC strongly recommends agencies use the services of the NLECC to obtain national interoperability keys, because it is the recognized national authority on encryption for public safety and maintains reliably strict and consistent procedures for generating, distributing, and managing keys. More information about the **NLECC: The Role of National Standards and Organization** can be found on page 29.

The NLECC sends encryption keys to agencies with an appropriately configured key fill device (KFD) or KMF through an NLECC approved interface. The agencies then use their KFDs to distribute the keys to individual subscriber units, either by directly connecting each unit to the device or transmitting the keys over the LMR network using OTAR. Encryption keys should not be distributed using a device with any wireless (Wi-Fi, Bluetooth) capability enabled, as this presents a security risk, and the NLECC does not distribute keys to any device whose wireless capability is enabled.

Encryption keys should be changed on a regular schedule determined by the security needs of the agency. They also should be changed if the security of the specific system channels or talk groups

is compromised, for example if an encrypted radio is lost or stolen or a third party or someone within the organization has intentionally or inadvertently shared one or more encryption keys with unauthorized persons.

By mutual agreement and through appropriate procedures, agencies may share encryption keys with neighboring agencies and mutual aid partners. All agencies participating in such a sharing agreement must adhere to a common set of security policies and practices. Keep in mind, however, that not all LMR radio vendors offer systems with the features and functions required to make key sharing practical. Therefore, procurement requests and requirements should be very specific and detailed describing how encryption services are to be used, shared, and managed to meet the operational requirements of the agency and its partners.

You will find specific guidance in the **Best Practices for Encryption Key Management** section of this document.

AES: A Built-In Advantage of Project 25

Many public safety radio systems are designed in compliance with the P25 standards, which optimize interoperability. P25 standards include AES256,[2] which is endorsed by NIST and embraced by industry and the cryptographic community.

Some readers may be familiar with the Data Encryption Standard (DES) algorithm, which NIST developed in 1977. In 1997, the Electronic Frontier Foundation cracked DES in 84 days of brute force computing. DES was cracked again in 1998 and twice in 1999, each time in fewer and fewer days. Since then, with the advent of more powerful computers, the time required to crack the DES algorithm has been reduced to hours.

Given the weakness of the DES algorithm, NIST withdrew its approval of DES and its derivatives as an encryption standard in 2005 and endorsed AES. Unlike the 56-bit length encryption keys used by DES, AES has an encryption key length of up to 256 bits,[3] enabling it to provide the most secure encryption available to the public safety community.

Today the P25 standards body has begun the task of removing DES from the various standards documents where it appears as they come up for review. For example the DES Encryption Protocol Standard and the DES Encryption Conformance Standard ceased to be P25 standards in October 2006 and June 2013, respectively.

---

[2] AES or Advanced Encryption Standard is described in Federal Information Processing Standard (FIPS) 197, NIST. FIPS 140-2 outlines how AES is applied to cryptographic modules in radio systems.

[3] A 256-bit string of random code presents 2^{256} potential solutions, or 115.7 followed by 76 zeroes. Using brute force calculation, today's most sophisticated computers would take many thousands if not millions of years to try every solution.

Models for Encryption Strategies

Implementing encryption while maintaining interoperability is a challenge. Encryption purposefully blocks specific communications while interoperability opens communications. How does an agency reconcile the two? Methodical planning and close coordination among all stakeholders eases the difficulty. For example, in the Washington, D.C. National Capital Region (NCR), the NCR has created a Strategic Regional Encryption Plan, with common radio zones, where encryption keys are shared among agencies with different response capabilities. The plan enables response coordinators to pick needed disciplines from D.C., Maryland, and Virginia jurisdictions and know that they will be able to communicate and coordinate on site—all on shared encrypted channels.

Practices for Successful Encryption Programs

Successful encryption programs share certain traits. Among them, the agencies with robust encryption strategies have:

- Identified and thoroughly examined encryption needs, including:
  a. types of information requiring encryption
  b. agency disciplines and talk groups that would benefit most from encryption
  c. mutual aid partners and other local, state, and federal agencies considered in an encryption strategy
- Involved in the earliest planning stages those experts within their organizations who could provide technical guidance regarding:
  a. scale of encryption effort
  b. required resources
  c. cost projections and options
  d. potential technical challenges and mitigations
- Convened potential end users of the technology—law enforcement, fire service, emergency medical, and emergency operations personnel—to gather views on:
  a. encryption needs
  b. how the planned encryption system might benefit operations
  c. potential obstacles encryption might pose to operations
  d. which features of the encrypted system would be most useful and which might be an unnecessary expense
  e. suggestions and recommendations to accommodate both intra-agency and interagency/mutual aid partner operations
- Discussed face-to-face with neighboring jurisdictions and mutual/automatic aid partners:
  a. perceived needs for encryption

   b. systems' encryption capabilities
   c. recommendations for encryption key sharing and management
   d. a structure for developing mutual policies, procedures, and governance for a shared encryption strategy

- Explored vendor options to identify offerings that:
   a. met the specific needs of the agency and its partners
   b. balanced cost and anticipated value
   c. included all necessary hardware, software, implementation, and warranty costs
   d. provided reasonably priced updates and upgrades, as needed
- Presented to their legislators or other state, local or tribal decision-makers:
   a. justification for investing in encryption, based on community and responder needs
   b. analyses demonstrating the anticipated benefits to public safety
- Researched funding options, including:
   a. federal grants
   b. cost sharing with local jurisdictions and state entities
   c. special taxes and/or assessments
- Held public forums to explain:
   a. the operational need for encrypted sensitive communications
   b. how encryption works
   c. steps taken to ensure legitimate public access to information

What About Legitimate Public and Media Access?

The need for public transparency is an important aspect for all public safety operations. Providing the public and the media with the information they want can conflict with an agency's operational needs. While the media themselves are liable for the consequences of reporting sensitive information protected under law, the primary responsibility for guarding such information lies with public safety agencies. Release or exposure of information can compromise criminal investigations and emergency responses or endanger lives or property, which is a primary consideration in the use of encryption.

Many jurisdictions achieve the balance of protecting critical information, while providing enough details to inform the public through their public information offices (PIOs). PIOs maintain public-facing websites and social media feeds and provide single points-of-contact for media outlets. They also have expertise in legal issues regarding public access to public safety information. It is strongly recommended that agencies include their PIOs, legal counsel, and risk managers in discussions about encryption to better serve the public and media in transmitting information for public use.

What About Cost?

Many agencies cite cost as a primary obstacle to encrypting radio traffic. While encryption may add expense to radio system and peripheral equipment procurements, setup, and maintenance, the cost is below what is commonly reported in the press. Factors that influence the cost of encryption include method of encryption, size of the system, numbers of peripherals, operational costs, and what is involved in distributing, securing, and maintaining encryption keys.

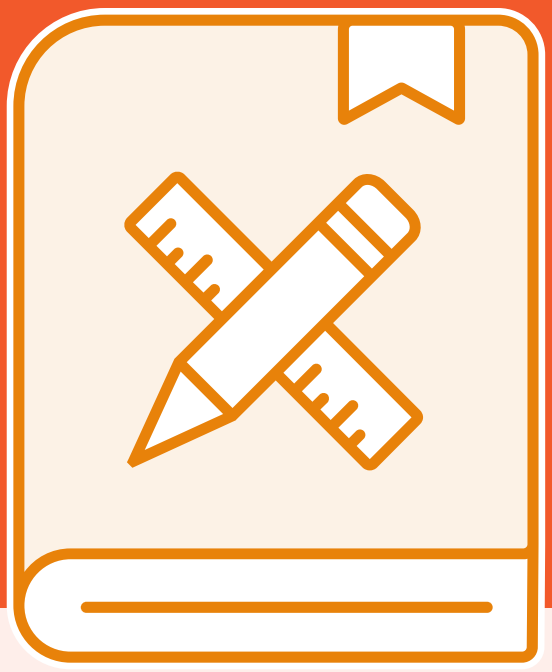
The cost can be difficult to justify in lean financial times; however, a careful risk assessment that weighs the cost of encryption against the potential impacts of not encrypting can provide convincing justifications. After extensive risk analyses, the U.S. Government had its justification and mandated that federal agencies implement encryption that complies with the NIST Federal Information Processing Standard (FIPS) 197, 140-2/140-3 and the 2002 Federal Information Security Act. Clearly, encryption when properly implemented is worth the cost.

Agencies without sufficient encryption technologies open themselves up to vulnerabilities that outside threat actors can exploit. These vulnerabilities could be far more costly to triage and recover from than purchasing and maintaining the appropriate encryption technologies. These vulnerability exploits could include:

- Identity theft and PII breaches
- Disruption of critical services
- Inability to provide necessary and timely services for the public's safety
- Breaches and tampering of ongoing criminal investigations
- Tampering of municipal or government records
- Increased operational risk to law enforcement officers and other public safety personnel
- Reduction of public trust
- Holding critical infrastructure and information for ransom
- Increased exposures to legal claims of wrongly death, injury, or criminal damage

In order to find the optimal level of encryption, agencies need to do their own cost benefit analysis to best position themselves to protect their communications systems and personnel. While many public safety officials and communications system administrators recognize the importance of encryption, they admit being confused by conflicting information about voice and data encryption in the LMR environment. This confusion makes decision-making difficult. This section addresses some of that confusion by focusing on the most important decisions and providing accurate, reliable information about the options available.

Guidelines for Making Good Technology Choices



Choosing an Encryption Algorithm

An encryption algorithm is the core of an encryption strategy. Choosing the algorithm that best suits an agency's needs today and in the foreseeable future establishes a solid foundation for everything that follows. Choosing a suboptimal algorithm or one that falls short of future needs condemns the agency to doubts about security and added costs for later upgrades. Several encryption algorithms are used in LMR systems throughout the U.S. As the section above (**AES: A Built-In Advantage of Project 25**) explains, one algorithm is more robust than any other available to public safety for mission critical LMR communications: the Advanced Encryption Standard (AES). AES offers a high level of security and, because it is integral to the P25 standards, offers a high level of interoperability.

While key lengths of 128 bits and 192 bits are authorized for use in AES, the Project 25 Block Encryption Protocol[4] strongly recommends a 256-bit key in public safety wireless systems. Current SAFECOM Grant Guidance[5] requires NIST-Compliant AES256 in P25 public safety systems when any encryption is procured and federal grant funds are used for the procurement.

While AES256 is strongly recommended, public safety leaders and system administrators should be able to explain to decisionmakers why competing encryption algorithms are inadequate. The two primary competitors in the marketplace are the archaic DES algorithm and various non-standard algorithms offered by specific manufacturers.

- **DES.** DES is described in the previously referenced section (**AES: A Built-In Advantage of Project 25**). Developed in the mid-1970s to protect U.S. Government communications, it was compromised years ago. Consequently, NIST withdrew certification for its use in U.S. Government applications, and DES has been removed from the P25 standards.

  While AES256's primary advantage is strong security, its position as the encryption standard throughout government, business and industry, and its status in the P25 suite of standards, make it the only reasonable choice for preserving interoperability. Practically all federal public safety agencies have upgraded to AES256 for voice and data encryption. Interoperating among federal partners on encrypted channels during a response operation requires the use of AES256. However, federal agencies regularly report difficulties with encrypted interoperability during operations when participating state, local, tribal, and territorial agencies do not have the AES256 capability.

  In February 2021 the International Association of Chiefs of Police (IACP) issued a resolution[6] stating "IACP strongly urges public safety agencies choosing to encrypt voice

[4] Block Encryption Protocol is described in the TIA technical document TIA-EIA-102.AAAD. It can be found at: https://archive.org/details/TIA-102_Series_Documents/TIA-EIA-102.AAAD_Block_Encryption_Protocol/

[5] *SAFECOM Guidance on Emergency Communications Grants* can be found at https://www.cisa.gov/sites/default/files/publications/FY%202021%20SAFECOM%20Guidance_Final_508.pdf

[6] IACP, Support for Police Use of National Institute of Standards & Technology (NIST)- approved AES Encryption Standard(s) in Voice and Data Communications, February 4, 2021

and data communications to choose the NIST-recommended AES suite for their future evolved encryption schemes, and require AES encryption standards appropriate for their application in all requests for information and requests for proposals" and "strongly recommends public safety agencies adopt the AES256 standard for police LMR operations and where appropriate, for use on Federal Communications Commission (FCC)-licensed channels specifically set aside for encrypted interoperability."

Considering the strengths and high-level endorsements of AES, several public safety agencies across all levels of government are calling for the "sunsetting" of DES. Many see this step as the best way to ensure standardization of encryption and avoid unnecessary obstacles to interoperability.

- **Proprietary/Unapproved Algorithms.** Proprietary algorithms offered by some manufacturers and other algorithms that have not been approved by accredited technical standards development organizations through standard testing protocols may not provide adequate protection regardless of their advertised key lengths. Without rigorous third-party testing, there is no way to know if an algorithm is as secure as its developer claims. Also, proprietary encryption limits interoperability to only those radios and systems that use the same encryption protocol. Again, because federal departments and agencies are required to use encryption that meets NIST standards—predominantly AES256—many state and local agencies are following their lead. Therefore, adopting a nonstandard encryption protocol could lead to difficulty communicating with federal, state, local, tribal, and territorial partners during an emergency.

Table 1. Algorithm Use Matrix

Algorithm	Key Length (bits)	Recommended Use
AES	128, 196, 256	Sensitive But Unclassified data All secure public safety communications
DES and all derivatives	56	No longer permissible or recommended for use
Non-standard-manufacturer/vendor offered proprietary solutions	Varies	Not recommended

Symmetric Encryption Keys

Symmetric encryption systems use the same key for encryption and decryption. Both the transmitting device and the receiving device contain the same key. AES uses a symmetric key system. Algorithms are extremely secure, but when shared keys are compromised—leaked to unauthorized persons or lost with an encrypted radio—they are usable by anyone. For this reason, in symmetric key systems the keys should be changed regularly and whenever a potential compromise is detected.

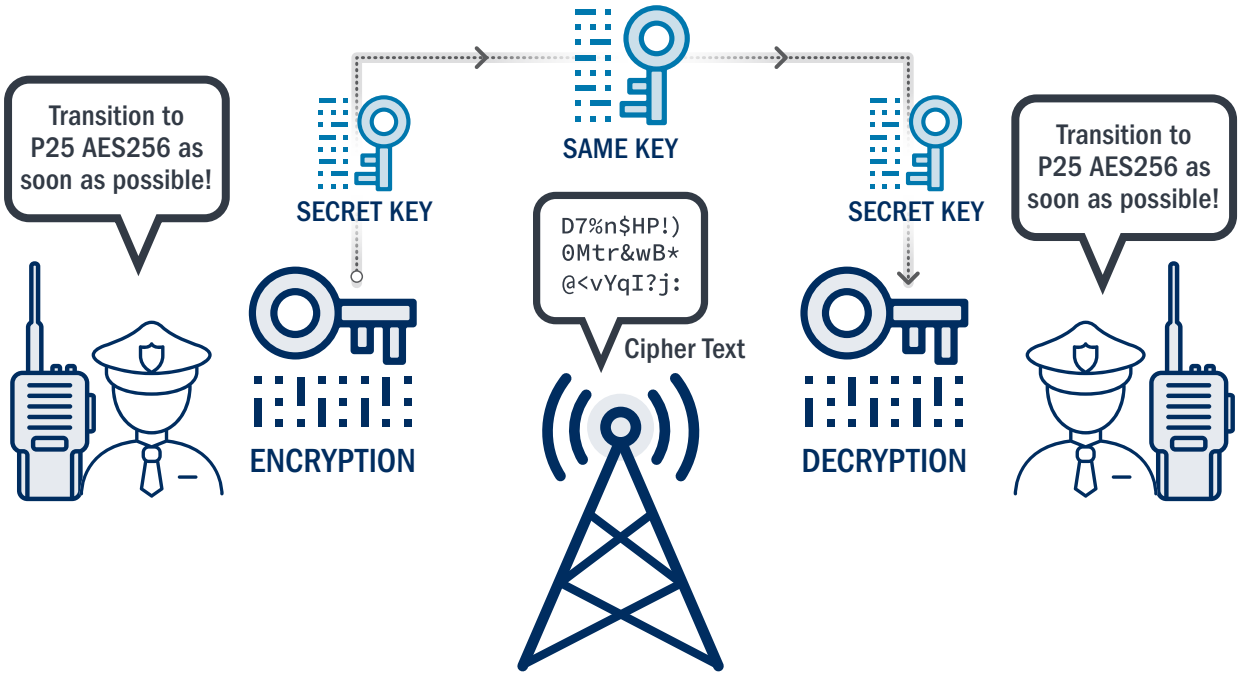


Figure 2. Symmetric encryption

NIST Validated Cryptographic Modules

Federal agencies using encryption for Sensitive but Unclassified (SBU) uses are required to utilize cryptographic modules validated by the NIST. The Cryptographic Module Validation Program (CMVP) employs independent third-party accredited security testing laboratories to validate the effectiveness of the security provided by a given cryptographic module. Validated modules provide a variety of security functions and the CMVP assigns each function a rating of 1 (lowest) to 4 (highest).[7] The cryptographic module is then given an overall security level, which is equal to the lowest level of any individual security function. It costs more money for manufacturers cryptographic modules to

[7] For a detailed understanding of security levels, see: FIPS 140-2 (nist.gov). Note: FIPS 140-2 has been superseded by FIPS 140-3. All new cryptographic modules will be validated under 140-3, and should manufacturers choose to revalidate they may do so under these new criteria.

get validated but improves cybersecurity profile and ensures mission integrity for the end users.[8] It should also be noted that any changes to the module requires revalidation.

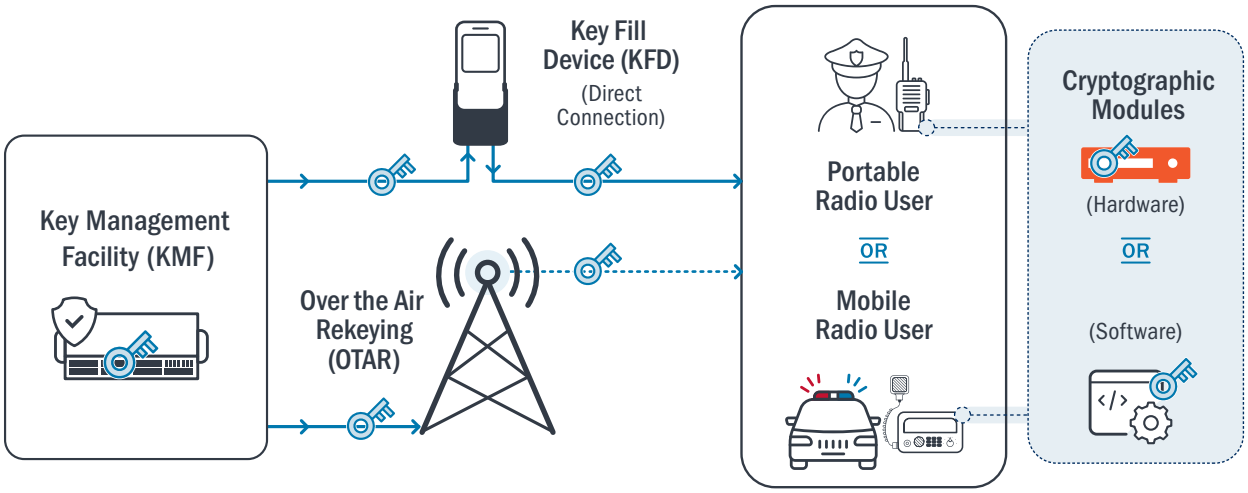


Figure 3. Cryptographic Module

NIST validated cryptographic modules can be implemented in hardware or software. In general, hardware modules achieve higher security levels than software. The majority of P25 LMR equipment is available with hardware validated encryption modules, although some lower tier equipment is now available with software validated modules. In nearly all cases, encryption is an optional feature and if it is not initially ordered with the required hardware module, adding encryption after delivery might result in higher cost.

It is recommended that all radios and radio systems interoperating in an encrypted environment utilize NIST validated cryptographic modules. Agencies should review and select the appropriate functional or overall rating that best meets their end user requirements.

Interoperability Considerations

Over the past two decades, public safety agencies at all levels of government have worked hard to establish interoperability among in-house disciplines and with surrounding jurisdictions and other mutual aid partners. The implementation of encryption sometimes appears as a serious threat to this progress. Preserving interoperability is simple if any agency and its partners all adopt the AES algorithm for wireless encryption. Yet what do agencies do if the jurisdictions around them, with whom they have mutual aid agreements, use DES or proprietary encryption protocols? What if local

[8] Validation is the responsibility of manufacturers and generally takes 12 months or more to complete.

partners have no encryption in place? If agencies implement encryption, how can they preserve interoperability with them?

The solution lies in meeting with mutual aid partners—one-by-one or together—and discussing the mechanics of all mutual operational and encryption needs; identifying the various communications technologies each agency uses; scrutinizing budget realities; identifying common goals and then researching the most practical technical solutions to meeting those goals.

Most encryption practitioners report surprise at the level of cooperation and problem solving generated by such meetings. Partners who never considered encryption become aware of the value. Partners who usually leap for the stars with technology temper their expectations to preserve interoperability. Goals are set. Experienced practitioners nearby and across the country are consulted. Research on budget solutions begins. Grant applications are drafted and submitted. It is a lot of work, but the potential of creating a solidly secure communication system that is fully interoperable is hard to resist.

For guidance, contact the FPIC at FPIC@cisa.gov.

Best Practices for Encryption Key Management

Introduction

By the time you reach this point in the document, you should have a sense of the importance of encryption. An agency can adopt an AES256-bit system, purchase top-shelf equipment that incorporates multi-key AES capabilities, contract with the NLECC to provide secure keys, and work out Memoranda of Understanding (MOUs) with cross-jurisdictional and other mutual aid partners, and still lose the game.

How? By not paying adequate attention to *encryption key management*.

An encryption key is akin to a personal Social Security number, bank account passcode, the password to electronic medical records or home Wi-Fi, but on an agency-wide scale. The loss of an encryption key can cripple sensitive operations, threaten the personal safety of colleagues, and reveal PII and PHI of private citizens, which could not only embarrass them but damage their careers and personal lives.

This section explores the basic elements of managing encryption keys for an LMR system. The emphasis is on best practices, illustrated with case studies that underscore what is at stake. It is based on the *Operational Best Practices for Encryption Key Management*[9] document developed by the FPIC, SAFECOM, and the NCSWIC in partnership with the NLECC, NIST, and subject matter experts from federal, state, local and tribal agencies nationwide. These are people who know encryption and its management.

Basics of Key Management

Key management covers every stage in the life cycle of an encryption key, from generating the key and assigning it an SLN slot, to keeping careful records of which radios and users have it, following policies and procedures to ensure both security and interoperability, setting a schedule for deactivating it, and taking steps to prevent a lost or stolen radio from compromising the entire encryption ecosystem. General information on how encryption works, the importance of using the AES256-bit algorithm, and organizing to develop an encryption strategy are found in the sections of this document beginning on page 15. This section assumes an agency has decided on a strategy and is ready to develop a key management system.

NLECC: The Role of National Standards and Organization

Because information and communications security is a national priority and LMR encryption is used extensively by federal, state, local, and tribal agencies, the NLECC has evolved to supply a uniform

[9] Operational Best Practices for Encryption Key Management is available at https://www.cisa.gov/sites/default/files/publications/08-19-2020_Operational-Best-Practices-for-Encryption-Key-Mgmt_508c.pdf

system for generating, distributing, supporting and managing encryption keys. The NLECC generates and distributes national interoperability keys and unique encryption keys for individual agencies and maintains a database of assigned keys to prevent key overlap and conflicts among agencies. It also supplies short-term voice and data encryption keys for special operations.

The NLECC manages the National Storage Location Numbers Assignment Plan, which provides a common configuration for storage location numbers (encryption key slots) in LMR subscriber units. The plan reserves SLN 1-20 for specific interoperability encryption keys, ensuring that federal agencies and their state, local, and tribal partners have a uniform configuration to ensure interoperability. The Recommended National Reserved SLN Table can be found in **Appendix B – The National Storage Location Numbers Plan Table** of this document.

In most cases, agencies seeking interoperable encryption keys from the NLECC must execute an MOU that outlines each organization's roles and responsibilities. The NLECC then configures and tests the agency's KMF/KFD(s) to ensure they meet key management requirements. The agency must ensure proper protocols are in place to securely disseminate the keys only to authorized equipment and protect them from unauthorized access. The NLECC requires the agency to notify them if any equipment containing encryption keys is lost or stolen so they can take necessary mitigation steps.

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

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

It is strongly recommended that agencies use the services of the NLECC for generating and managing nationwide or regional interoperability encryption keys and adhere to the National Storage Location Numbers Assignment Plan when assigning keys to their radios.

The National SLN Plan: Lesson Learned

A county with a P25 radio system wanted a federal agency to join its network for interoperable encrypted communications. The organizations agreed to have federal agency subscriber units affiliate with the county KMF for key management and distribution. Yet when programming the radios, technicians discovered the county had not coordinated its SLN assignments with the NLECC and had programmed its own agency-specific keys in the reserved SLN slots 1-20. The programming conflicts prevented sharing encrypted communications. The county had to implement a time-and resource-intensive reprogramming initiative to correct the issue so it could have encrypted communications with the federal agency and others in the future.

Key Transmission Guidelines

The NLECC distributes encryption keys to agencies through secure connections to the agencies' KFDs and requires agencies to disable any wireless capabilities in those devices. A KFD whose Wi-Fi or Bluetooth capabilities are disabled is referred to as hardened. Hardening ensures that the KFD does not inadvertently "leak" the encryption keys onto a wireless network where unauthorized individuals could access them.

Agencies, in turn, distribute the keys to their subscriber units. There are two ways to do this: 1) connect each subscriber unit manually to the KFD or 2) use OTAR. OTAR is an optional feature on multi-key radios that enables agencies to distribute keys securely over the radio network. Using OTAR, agencies can update, replace, or disable keys in all OTAR capable (multi-key) subscriber units in its system. A KMF or access/affiliation to a KMF on another system is necessary to effectively use OTAR.

Figure 4 illustrates the risk in distributing keys without adequate security measures. In the figure, Wi-Fi enabled devices present vulnerabilities that could allow unauthorized users to intercept the transmission of encryption keys. Such vulnerabilities pose a threat to not only the encryption system of the agency itself but to the systems of mutual aid partners who share its keys.

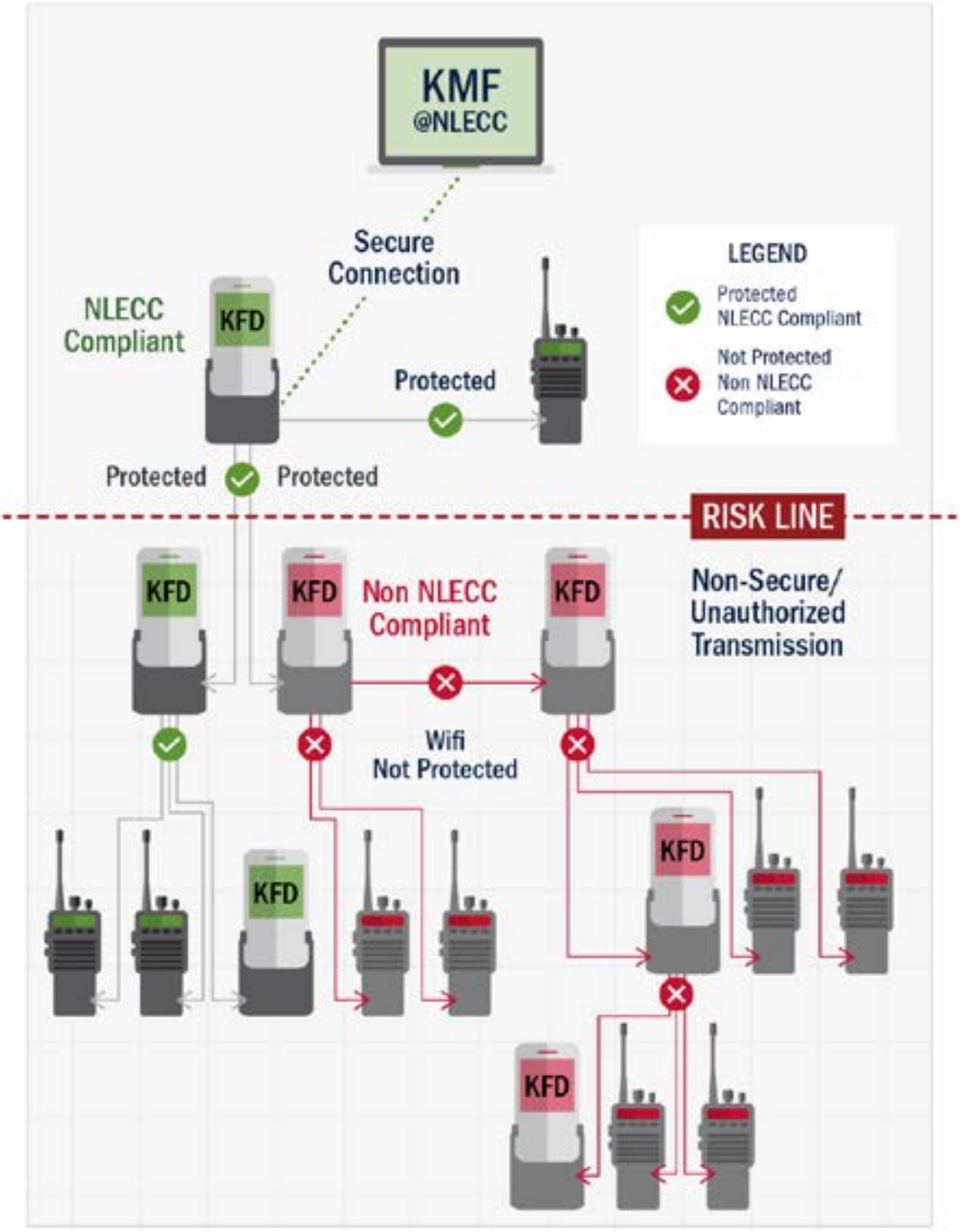


Figure 4. Security risk when a Wi-Fi enabled device is used for cryptographic key distribution

If procuring KFDs, agencies should make sure these devices are standards compliant and incorporate a hardware security module and are not just laptop computer and cables.

Case Study #1: Coordinating Secure Key Distribution Among Agencies

A county EMS division realized addresses and patient information for 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 AES256-bit encrypted, trunked radio system talk group operated by the county. The EMS agency licenses 47 emergency medical Advanced Life Support (ALS) providers for ALS radio contact, including fire departments, private ambulance companies, sheriff SWAT teams, and aero-medical services. Sixteen hospitals use the system to communicate with field units.

Recordkeeping and KFD Security

Key management was assigned to the sheriff's department, which decides which keys will be used and the OTAR schedule for updating keys. At monthly EMS agency/stakeholder meetings, the department shares the date and time of OTAR events at least two months in advance to give each stakeholder time to plan for the update. The time of day (usually early morning before the daily paramedic-hospital radio check) is chosen to enable radio users to make sure the OTAR is successful ahead of the day's operations. Agencies without OTAR-capable radios are given more time to manually rekey their radios 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.

As in all areas of management, recordkeeping for an encryption system is essential. System administrators must keep accurate, up-to-date records of who in their organizations have encrypted radios and what keys and talk groups are assigned to those radios. Keep track of all organizations with whom an agency shares keys and confirm with the NLECC that those organizations are authorized to receive keys from the NLECC. Be meticulous about recording changes to these records, and regularly verify that radios are in the possession of the personnel to whom they are assigned.

Keep close track of KFDs. These are the distribution hub for encryption keys, and any unauthorized personnel accessing them could intentionally compromise the entire encryption ecosystem. All personnel with access to KFDs, especially third-party contractors, should be properly vetted and carefully monitored. Keep detailed records of where KFDs are located and who is responsible for them, especially if the devices are used off-site or taken to various facilities to manually key LMR subscribers or console equipment.

Case Study #2: Losing Control of a KFD

A municipality noticed a significant increase in local drug trafficking and related crime. Investigators received actionable leads yet failed when attempting street arrests and staging

raids on suspected drug dealers' homes. Eventually they discovered the criminals had identified a radio shop employee with access to KFD and used this employee to load keys onto the municipality's radio system and subscribers. The employee accepted bribes to load the police department's cryptographic keys into the criminals' unauthorized radios, enabling them to actively monitor the narcotics unit's encrypted communications and avoid planned raids and other surveillance operations.

How to Handle Lost and Stolen Encrypted Radios

Losing any subscriber unit or other piece of communications equipment is serious. Replacements are expensive. The situation is even more serious when an encrypted radio disappears because it holds encryption keys whose loss can compromise the entire communications system, endangering sensitive operations and threatening personnel safety.

NLECC policy requires agencies to report the loss of any radio holding NLECC-issued cryptographic keys. This policy ensures compromised keys can be deactivated promptly. If an agency generates its own encryption keys, the policies and procedures should require the reporting of lost or stolen radios as soon as possible—certainly within 24 hours. Through periodic repeatable radio training, public safety personnel must be made to understand that reporting a missing subscriber unit immediately is paramount. Knowing you have a problem is the only way to resolve that problem in time to avoid consequences.

Case Study #3: Reporting Lost or Stolen Devices

A local law enforcement agency conducting an ongoing drug operation suddenly found its apprehension rate dropping significantly. A confidential informant revealed the criminals had found an agency subscriber unit and were using it to eavesdrop on investigative and tactical communications. The agency immediately disabled the stolen radio remotely and changed the encryption keys in all agency devices. Drug seizures and apprehensions noticeably increased.

Case Study #4: Decommissioning of LMR Equipment

An alarming trend has been observed nationwide where agencies are disposing of surplus, end of life, stolen or lost equipment that has not been properly decommissioned. As agencies are preparing to dispose of equipment they must "zero out" the radio programming and encryption keys. Reference to the equipment in system databases should also be removed so that lost or stolen radios may no long affiliate to a system.

Maintaining Interoperability: Coordinating Encryption with Partners

Interoperability is the brass ring during multi-jurisdictional incidents. The ability of responders to communicate and coordinate seamlessly during critical response operations is key to saving lives and property and ensuring the safety of personnel. Unfortunately, encryption, as valuable as it is, can disrupt interoperability. But as encryption practitioners across the country indicate, it does not have to negatively affect interoperability. Encryption and interoperability can live peacefully and efficiently together.

What is needed is comprehensive planning and coordination among all the partners who want to share an encryption strategy and an operational plan. Meet with all current and prospective partners and define operational and encryption requirements, roles and responsibilities, schedules and plans, and ongoing or shared costs. A strategic element of the plan for proceeding collectively together must also be contemplated and as well as an agreement to meet the stated requirements. (See the section **"Models for Encryption Strategies"**.) Because different agencies and jurisdictions have diverse levels of resources and technical competency, these discussions can be difficult, but they are extremely useful.

Interagency operations requiring encrypted interoperable communications should implement MOU or Memoranda of Agreement (MOA) among partners, when practical, to formalize key management and governance processes. Formalization gives all partners a clear view of their roles and responsibilities and indicates the technology and training requirements they must provide for to actively and effectively participation.

Where formal agreements are inappropriate, organizations can agree informally on roles and responsibilities if there is clear understanding among them.

Case Studies #5 and #6: MOUs, MOAs, and Informal Agreements Among Mutual Aid Partners

A county sheriff's department approached the U.S. Coast Guard (USCG) about establishing encrypted communications to improve coordination during interagency operations. The sheriff's department had purchased radios with AES encryption, capable of being programmed with USCG very high frequency (VHF)-frequency modulation (FM) command and control channels. USCG provided 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. The parties drafted an MOA to document their respective key management roles, responsibilities, and processes. The MOA provided the sheriff's department with consistent, direct, encrypted communications with the USCG 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 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 staff of the various agencies developed an informal interoperability agreement through e-mail and phone calls to resolve the various technical challenges, including establishing and sharing secure interoperability keys. The operation was a success.

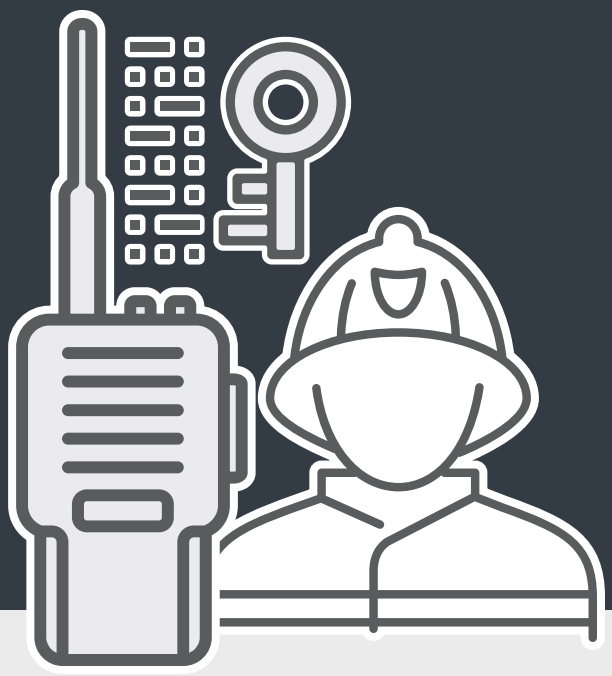
Grant Funding for Encryption Strategies

Federal grant funds are available to agencies for implementing an encryption strategy. This includes transitioning (planning, procurements of new/updated encryption equipment/services and implementation) to AES from other encryption algorithms. Funding resources and grant guidance are found on the SAFECOM Funding Resources webpage at cisa.gov/safecom/funding. Keep in mind that any equipment inclusive of encryption to be purchased with grant funds must also include P25 standards-based AES256-bit encryption as described in the TIA-102.AAAD-B, Project 25 Digital Land Mobile Radio Block Encryption Protocol[10].

Grant recipients should purchase equipment tested through the P25 Compliance Assessment Program (P25 CAP). This voluntary program enables LMR equipment suppliers to verify their equipment is P25-compliant through testing at a DHS-approved testing laboratory. Information on P25 CAP compliant devices can be found on the Approved (Grant-Eligible) Equipment page (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.

[10] Commercial entities version available at https://global.ihs.com/doc_detail.cfm?&item_s_key=00378220&item_key_date=840107&input_doc_number=TIA-102.AAAD-B&input_doc_title=. Government entities can request the document from http://standards.tiaonline.org/all-standards/p25-downloads-application.

Appendices



Appendix A – Basic Key Management Practices

BEST 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 compromises 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
- Limit number of keys available within a KFD
- Maintain the physical security and controlled access to KMFs and KFDs
- 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
- Maintain accountability and public trust reinvestigation of personnel
- When establishing encryption key procedures pay close attention to National SLN 1-20 assignment plan (**Appendix B**)

Appendix B – The National Storage Location Numbers Plan Table

* These algorithms are no longer authorized per the 2005 NIST withdrawal of the use of DES within the P25 standards. As of January 1, 2022 existing DES keys will remain available but no new DES keys will be generated and distributed.

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 Fed Law Enforcement Interoperability	FED CAN	Static	All US - Canadian Federal LE
8	AES	US – Canadian PS Interoperability	USCAN PS	Static	All US and Canadian PS 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

SLN	Algorithm	Use	SLN Name	Crypto Period	Authorized Users
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	FED Task Force
16	AES	National Task Force Operations	FED TF A	One time use as needed for Special OPS	FED 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
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 LE
20	AES	Public Safety – International Law Enforcement Interoperability	PS INTL	When needed by operational requirement	All US and Visiting International Public Safety

Appendix C – Contacts for More Information

Additional information about implementing and managing P25 LMR encryption systems, can be found here:

- 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-contact-information
- The Federal Partnership for Interoperable Communications Security Subcommittee: AESTransition@cisa.dhs.gov
- Emergency Communications Coordinators: https://www.cisa.gov/resources-tools/programs/emergency-communications-coordination-program

Appendix D – Reference Documents

This is a partial list of documents that readers may find helpful for learning about encryption and implementing encryption systems.

Security Requirements for Cryptographic Modules (FIPS PUB 140-3)
https://csrc.nist.gov/publications/detail/fips/140/3/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 4, Recommendation for Key Management Part 1: General
https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/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://csrc.nist.gov/publications/detail/sp/800-130/final

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 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

SAFECOM Guidance on Emergency Communications Grants
https://www.cisa.gov/safecom/funding