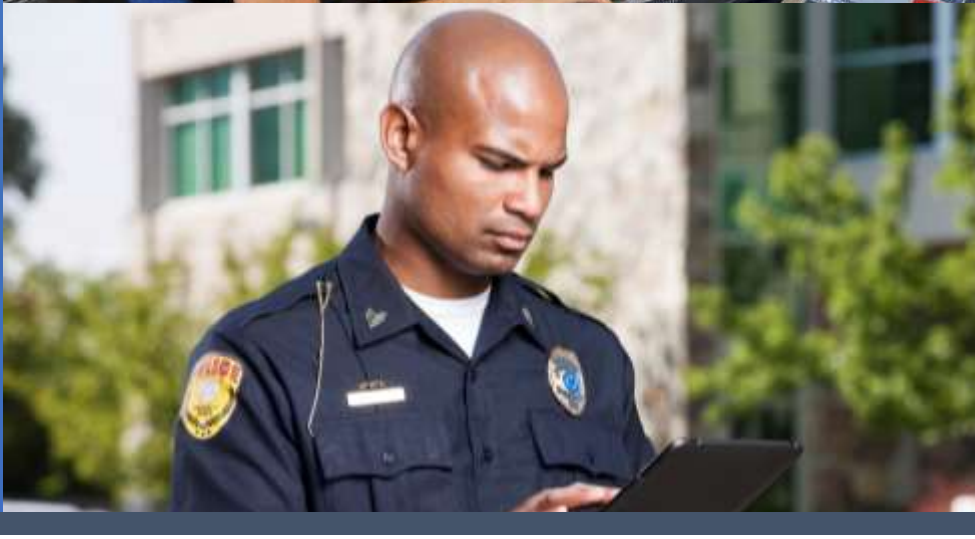


Technology Policy Resources

September 2016

SAFECOM

NCSWIC

Table of Contents

About SAFECOM and NCSWIC

Federal Partnerships for Interoperable Communications (FPIC) Encryption

T- Band Executive Briefing

About SAFECOM and NCSWIC

DHS OEC and the Joint SAFECOM and NCSWIC Funding and Sustainment Committee developed this document. SAFECOM's membership includes more than 60 members representing federal, state, local, and tribal emergency responders, elected and appointed officials, and major intergovernmental and national public safety associations, who provide input on the challenges, needs, and best practices of emergency communications. The NCSWIC is comprised of Statewide Interoperability Coordinators
(SWIC) and their staff from 56 states and territories; SWICs promote the critical importance of interoperable communications. This document reflects the expertise of SAFECOM and NCSWIC members, and DHS OEC coordination efforts to share innovative methods, best practices, and lessons learned in funding and sustaining public safety communications systems. The Joint SAFECOM and NCSWIC Funding and Sustainment Committee will continue to seek best practices for emergency communications grantees and share updates as they become available.

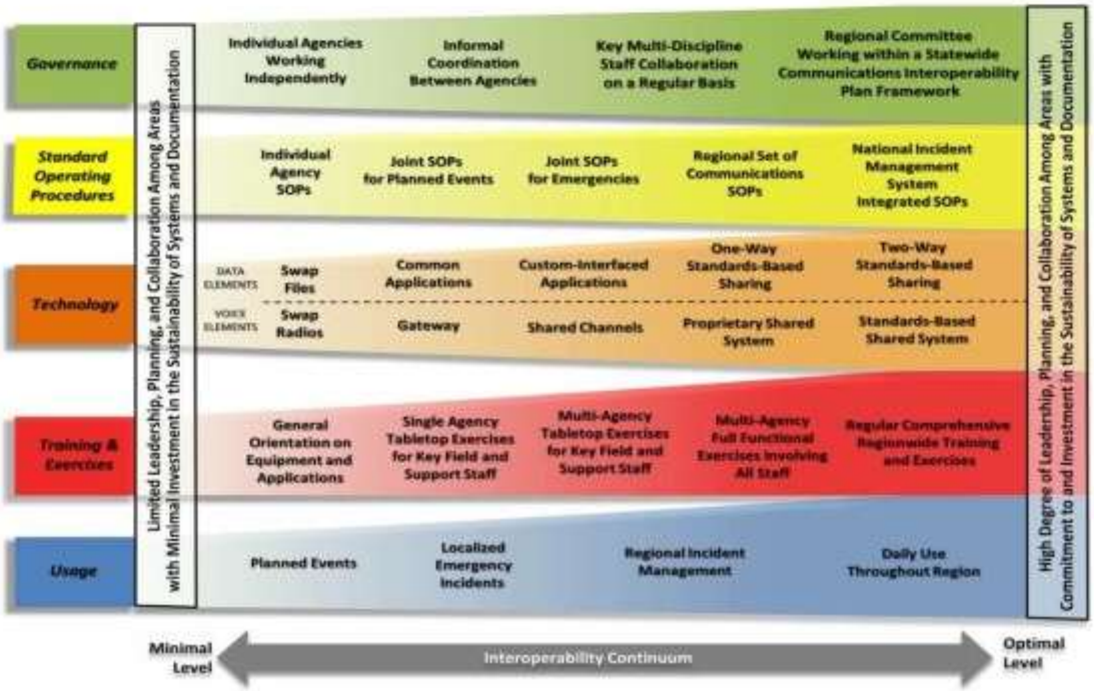
SAFECOM: www.dhs.gov/SAFECOM **NCSWIC:** www.dhs.gov/SAFECOM/NCSWIC

About SAFECOM and NCSWIC

SAFECOM Interoperability Continuum

Developed with practitioner input from the Department of Homeland Security's (DHS) SAFECOM program, the Interoperability Continuum is designed to assist emergency response agencies and policy makers to plan and implement interoperability solutions for data and voice communications. This tool identifies the five critical success elements that must be addressed to achieve a sophisticated interoperability solution: governance, standard operating procedures, technology, training and exercises, and usage of interoperable communications. The Interoperability Continuum can be used by jurisdictions to track progress in strengthening interoperable communications. In addition, the DHS Office of Emergency Communications has used the Interoperability Continuum to develop the priorities and measure the goals of the National Emergency Communications Plan.

Exhibit A5-1. SAFECOM Interoperability Continuum


Governance
Individual Agencies Working Independently
Informal Coordination Between Agencies
Key Multi-Discipline Staff Collaboration on a Regular Basis
Regional Committee Working within a Statewide Communications Interoperability Plan Framework
Standard Operating Procedures
Individual Agency SOPs
Joint SOPs for Planned Events
Joint SOPs for Emergencies
Regional Set of Communications SOPs
National Incident Management System Integrated SOPs
Technology
DATA ELEMENTS
Swap Files
Common Applications
Custom-Interfaced Applications
One-Way Standards-Based Sharing
Two-Way Standards-Based Sharing
VOICE ELEMENTS
Swap Radios
Gateway
Shared Channels
Proprietary Shared System
Standards-Based Shared System
Training & Exercises
General Orientation on Equipment and Applications
Single Agency Tabletop Exercises for Key Field and Support Staff
Multi-Agency Tabletop Exercises for Key Field and Support Staff
Multi-Agency Full Functional Exercises Involving All Staff
Regular Comprehensive Regionwide Training and Exercises
Usage
Planned Events
Localized Emergency Incidents
Regional Incident Management
Daily Use Throughout Region
Limited Leadership, Planning, and Collaboration Among Areas with Minimal Investment in the Sustainability of Systems and Documentation
High Degree of Leadership, Planning, and Collaboration Among Areas with Commitment to and Investment in the Sustainability of Systems and Documentation
Minimal Level
Interoperability Continuum
Optimal Level

Interoperability is a multi-dimensional challenge. To gain a true picture of a region's interoperability, progress in each of the five interdependent elements must be considered. For example, when a region procures new equipment, that region should plan and conduct training and exercises to maximize the use of that equipment. Optimal level interoperability is contingent upon individual agency and jurisdictional needs. The Continuum is designed as a guide for jurisdictions that are pursuing a new interoperability solution, based on changing needs or additional resources; it is an evolving tool that supports national preparedness doctrine including, but not limited to, the National Incident Management System, the National Response Framework, and the National Emergency Communications Plan. To maximize the Interoperability Continuum's value to the emergency response community, SAFECOM will regularly update the tool through a consensus process involving practitioners, technical experts, and representatives from Federal, State, local, and tribal agencies.

Summary of Technology Policy Committee Resources

The following materials were developed by SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) to help state and local stakeholders educate decision-makers and elected officials on emerging challenges to interoperable communications faced by public safety community. These documents can be used as read-ahead materials or handouts. All of the products listed below are available on the SAFECOM website.

Federal Partnerships for Interoperable Communications (FPIC) Encryption Suite
The Federal Partnerships for Interoperable Communications (FPIC)[1] Security Working Group (SWG) collaborated with SAFECOM, the Department of Homeland Security OneDHS Emergency Communications Committee[2], SAFECOM Emergency Response Council (ERC)[3], the National Council for Statewide Interoperability Coordinators (NCSWIC)[4], and the DHS Southwest Border Communications Working Group (SWBCWG)[5] to develop a series of guidelines, best practices, and considerations for public agencies looking to implement encrypted communications.

FPIC Encryptions Documents

- **Considerations for Encryption in Public Safety Radio Systems (Paper)** This document examines the complex issues of why encryption may be needed during critical operations of an urgent or time-sensitive nature or when open communications may not be sufficient to protect personally identifiable and/or sensitive information. This document is provides guidance to public safety users through a process to assess the need for encryption as well as the questions that must be considered.
- **Determining the Need for Encryption in Public Safety Radios (Fact Sheet)** This document provides a high-level overview of all the factors public safety agencies and department should thoroughly discuss and carefully considered before reaching a decision to encrypt their public safety radio systems.
- **Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems (Paper)** This document addresses methods to improve cross-agency coordination and emphasizes the use of standards-based encryption to enhance secure interoperability and minimize the risk of compromising sensitive information.

[1] The FPIC is recognized as a technical advisory group to SAFECOM and the ECPC and works to address technical and operational wireless issues relative to interoperability within the federal emergency communications community, as well as interfaces with state and local agencies. It includes more than 200 federal, State, local, and tribal public safety representatives from over 45 Federal agencies, as well as representatives from State, tribal and local entities.

[2] OneDHS worked to coordinate and integrate communications activity within DHS.

[3] SAFECOM was formed in 2001 after the terrorist attacks of September 11, 2001 as part of the Presidential E-Government Initiative to improve public safety interoperability, allowing emergency responders to communicate effectively before, during, and after emergencies and disasters. Although the ERC is no longer active, its former members comprise the overall SAFECOM membership.

[4] NCSWIC assists state and territory interoperability coordinators with promoting the critical importance of interoperable communications and the sharing of best practices to ensure the highest level of interoperable communications across the nation.

[5] SWBCWG serves as a forum for F/S/L/T agencies in Arizona, California, New Mexico, and Texas to share information on common communications issues; collaborate on existing and planned activities; and, facilitate federal involvement in multi-agency projects within the Southwest Border Region.

- **Developing Methods to Improve Encrypted Interoperability in Public Safety Communications (Fact Sheet)** This document highlights best practices of key management necessary to allow encrypted operability and interoperability. These best practices are important in developing system security where encrypted interoperability is realizable. Additionally, significant planning and coordination must be undertaken to achieve encrypted interoperability on a national scale.

T-Band Executive Briefing

The purpose of the T-Band Executive Briefing is to provide a list of high-level talking points to help interested public safety officials present an "elevator speech" to raise awareness of the primary challenges connected with the T-Band relocation issue.

SAFECOM and NCSWIC encourage you to share these documents with public safety agencies in your region. Stakeholders throughout the public safety community have already leveraged these documents to help inform officials of public safety needs, and for guidance to make informed procurement decisions. If you have any questions or feedback on these materials, please contact SAFECOM at SAFECOMGovernance@HQ.DHS.GOV or NCSWIC at NCSWICGovernance@HQ.DHS.GOV

Considerations for Encryption in Public Safety Radio Systems

September 2016

SAFECOM

Federal Partnership for Interoperable Communications FPIC

NCSWIC

Preface

This document was developed at the request of the public safety community to provide supporting information for consideration and decisions at all levels of government to encrypt critical portions of public safety communications systems. It is essential the design and operation of mission critical radio systems enable voice and data communications that is protected from unauthorized reception as required.

This document examines the complex issues of why encryption may be needed during critical operations of an urgent or time-sensitive nature or when open communications may not be sufficient to protect personally identifiable and/or sensitive information. It should be noted that there may be differing legal requirements in various jurisdictions relating to the encryption of communications on Public Safety radio systems. Therefore, when considering encryption, in addition to operational and policy considerations, a legal analysis should be conducted.

This report is a result of an extended effort by the Federal Partnership for Interoperable Communications (FPIC)[1] Security Working Group and other contributing individuals, agencies, and organizations outlined in Appendix B. The FPIC wishes to acknowledge the valuable input of the following groups and organizations: Department of Homeland Security OneDHS Emergency Communications Committee[2], SAFECOM Emergency Response Council (ERC)[3], the National Council for Statewide Interoperability Coordinators (NCSWIC)[4], and the DHS Southwest Border Communications Working Group (SWBCWG)[5]. It is important to note that there are significant governance, policy, and training implications that must be considered with the use of encryption. In addition, a *Fact Sheet* has been developed to accompany this document that provides a high-level summary of the key facts, issues, and recommendations for the encryption of public safety radio systems at all levels of government.

[1] The FPIC is recognized as a technical advisory group to SAFECOM and the ECPC and works to address technical and operational wireless issues relative to interoperability within the federal emergency communications community, as well as interfaces with state and local agencies. It includes more than 200 federal, State, local, and tribal public safety representatives from over 45 Federal agencies, as well as representatives from State, tribal and local entities.

[2] OneDHS worked to coordinate and integrate communications activity within DHS.

[3] SAFECOM was formed in 2001 after the terrorist attacks of September 11, 2001 as part of the Presidential E-Government Initiative to improve public safety interoperability, allowing emergency responders to communicate effectively before, during, and after emergencies and disasters. Although the ERC is no longer active, its former members comprise the overall SAFECOM membership.

[4] NCSWIC assists state and territory interoperability coordinators with promoting the critical importance of interoperable communications and the sharing of best practices to ensure the highest level of interoperable communications across the nation.

[5] SWBCWG serves as a forum for F/S/L/T agencies in Arizona, California, New Mexico, and Texas to share information on common communications issues; collaborate on existing and planned activities; and, facilitate federal involvement in multi-agency projects within the Southwest Border Region.

Executive Summary

We live in an ever-changing world, and the world is becoming a more complicated (and dangerous) place to live and work. This has caused public safety agencies to place greater importance on how it uses technology and how it enhances the ability to protect and serve. Since the terrorist attacks of September 11, 2001, public safety has had to rethink communications strategies to meet the challenges of this changing world. Today we find many public safety communications channels streamed across the Internet or openly broadcast giving the public, media, criminals, and potential terrorists immediate access to crucial public safety information. As agencies work to enhance interoperability, they also have to remain keenly aware of the need to protect critical public safety communications from compromise, so that information cannot be used to hinder emergency response, impede investigation and surveillance, or endanger the public. Public safety agencies should begin to think about protecting that information and consider how factors such as interoperability, cost, and complexity may be affected. As we design, upgrade, and implement public safety communications systems, protecting critical information should become part of the process.

Public safety radio encryption may be the best way to protect critical information transmitted over the airwaves from compromise and disclosure. There are a number of examples how encryption can help mitigate problems created by open or unauthorized listening to sensitive public safety information. Some recent incidents are illustrated in this document. They include active shooter incidents, public knowledge of sensitive public safety information, and the safety of personnel, the public and property. In addition, other generalized scenarios that involve Urban Search and Rescue, training, emergency response, active investigation and surveillance, personally identifiable information, and scanners/social media are discussed.

The implementation of encryption is an important policy decision that stakeholders, decision-makers, and leadership must carefully consider and plan. This paper explores the reasons, implications, and considerations associated with the decision to encrypt. As shown, encryption can significantly decrease the possibility that sensitive public safety information can be used to impede effective emergency response or jeopardize the safety of life and property. Undoubtedly, the policy and legal decision to encrypt can be complex, but the threat of the compromise of critical information to the safety of the public is clear.

Before decisions are made regarding when and how to encrypt, it is very important to consider what information should be protected. Although each jurisdiction or agency will likely have differing perspectives, the primary questions to be addressed will be fairly common. These questions 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 versus the impact of compromise?
- What is the effect on public information access?

All the factors discussed should be thoroughly and carefully considered before reaching a decision regarding encryption for a public safety radio system in a specific jurisdiction or discipline. Most Federal agencies continue to recognize the importance of encrypting public safety mission critical radio communications and understand encryption is vital to national security and mission integrity. State and local governments should consider 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?**

Considerations for Encryption

The District of Columbia Chief of Police, in a 2011 testimony, urged the city council to approve the encryption of their public safety radio system by stating it would "deter crime, as criminals have used scanners to track police activity and plan their crimes." She cited a number of cases where un-encrypted radios allowed criminals to intercept police radio transmissions and thwart law enforcement prevention of crimes. They included some carjacking incidents in 2010 and a drug operation run out of a public laundry.[6]

This example is somewhat typical of why many jurisdictions are implementing encryption within their public safety communications systems. They do not want criminals to be able to "scan" or listen to police radio communications and they want to be able to protect other sensitive information from unauthorized use.

There are thousands of radio systems either existing or planned for our Nation's public safety agencies. Many of these agencies combine local, regional, or statewide government communications needs into multi-jurisdictional or multi-discipline systems, often integrating functions such as public safety, public service, maintenance, and administration into a single radio system. Although all of these functions are not generally critical to the safety of life, they *do* support law enforcement, firefighting, and emergency medical missions. Those missions often involve:

- Safety of personnel, and enhanced safety of the public and property,
- Sensitive law enforcement information including active investigations and surveillance,
- Personally identifiable information (PII, Sensitive PII and/or protected health information (PHI) privacy act or health privacy data),
- 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[7]," leaving little protection from monitoring by someone with a basic knowledge of radio communications and fairly simple equipment. Interception of all public safety radio traffic is unlikely, but the compromise of some information can be problematic and may jeopardize safety and mission integrity.

The use of encryption helps manage the risk to personnel safety and protection of sensitive information. Each agency must assess the risk of *not* encrypting radio traffic against the potential effect of that traffic being intercepted. If the impact is insignificant, then the risk may be acceptable. An example might be the "clear" transmission of administrative traffic involving

[6] DCist.com, Nov 7, 2011.

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

maintenance, transportation, or other non-mission critical information. In this case, that information is generally not critical. On the other hand, the impact of not protecting more sensitive information and potentially divulging that information to someone who is not authorized to receive it or who might use that information for criminal activities might be life-threatening or extremely detrimental to the safeguarding of property.

The best way to attempt to protect sensitive information and to ensure that public safety personnel and operations are protected from unwanted disclosure is to encrypt part or all of the radio traffic. Encryption provides the assurance that this sensitive information can be reasonably safe from unwanted use.

What is Encryption and how does it protect critical information?[8]

In a radio communications system, encryption is a means of encoding radio transmissions in such a way that only the person or system with the proper key[9] can decode it. An encryption algorithm or cipher "codes" the information to such a degree that it becomes extremely difficult to listen to radio transmissions without authorization, the proper decoding equipment, and the correct key. Many public safety radio systems today are digital and designed in compliance with applicable industry standards such as Project 25 or P25[10], which improves interoperability between radio systems. The P25 standard includes a strong encryption method known as the Advanced Encryption Standard, or AES[11]. AES is a standard created by the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce. Project 25 selected AES, with a 256 bit key length (AES-256), as the primary encryption algorithm for interoperability. With the use of P25 AES, public safety agencies can provide the best, currently available protection for their radio traffic to attempt to assure it is protected against unauthorized access. Although the Data Encryption Standard (DES) is still utilized for interoperability, agencies are strongly encouraged to migrate to AES due to the known vulnerability of the older algorithm (DES). Importantly, encryption techniques and algorithm deployments ***other than AES-256*** are vulnerable to compromise.

[8] Detailed information regarding encryption for public safety radio systems can be found in the SAFECOM – NCSWIC – FPIC publication: *Guidelines for Encryption in Public Safety Radio Systems*, February 2016, which can be found at http://www.dhs.gov/technology.

[9] An encryption key is a parameter that allows the encryption algorithm to function effectively. It literally "locks" and "unlocks" protected information

[10] Project P25 (P25) is the standard for the design and manufacture of interoperable digital two-way wireless communications products. Developed in North America with state, local and federal representatives and Telecommunications Industry Association (TIA) governance, P25 has gained worldwide acceptance for public safety, security, public service, and commercial applications.

[11] AES or Advanced Encryption Standard is described in Federal Information Processing Standard (FIPS) 197, National Institute of Standards and Technology. FIPS 140-2 outlines how AES is applied to cryptographic modules in radio systems.

Examples of Why Encryption is Desirable

An effective way to illustrate that encryption of public safety land mobile radios is desirable is to discuss the risk and consequences of *not* encrypting radios. The incidents below illustrate why encryption has become a preferred means for the safety of personnel and the protection of sensitive information. Additionally, a number of scenario-based incidents and other considerations that can be affected by the decision to encrypt are listed and described in more detail in Appendix A.

Specific Examples based on actual incidents:

- **Ft. Hood Active Shooter –** The tragic shooting at Ft. Hood, Texas on April 4, 2014 further illustrates the need to encrypt sensitive law enforcement communications. At 5:57pm the discussion began on the popular website reddit.com[12]. The first item to be posted was the link to the live feed of the local public safety agency[13]**.** Within a few minutes an update was posted that announced the first shooter was down and the police were looking for a second suspect driving a late model Toyota Camry armed with a .45 caliber handgun. Minutes later someone posted that the second suspect is "at large" wearing an army combat uniform. The first ten minutes of the scanner audio was even posted to YouTube[14]. This was from one social media site. There were others that exploited this information, potentially hindering emergency response. In this age of instant access to information it is essential to the successful outcome of any situation that requires public safety response to control the means of mission critical communications and to ensure tactical information is not disseminated for everyone to hear.

- **Phoenix, Arizona –** In January 2013[15], the Phoenix Police broadcast the location of a shooting suspect's home, alerting the media and causing the suspect to flee prior to police apprehension. Other incidents in Phoenix have complicated investigations and allowed public access to criminal information of minors, as well as tactical information regarding stakeouts and criminal investigations including incidents involving juveniles, fugitives from justice, and compromise of tactical positions and response. These incidents caused the Police Department to encrypt a portion of their radio traffic to enhance officer safety and protect sensitive law enforcement and personal information.

- **Fort Collins, Colorado –** In 2013, the Fort Collins Colorado Police Department[16] began encrypting all routine radio traffic so the public could not listen with scanners or

[12] (http://www.reddit.com/r/news/comments/221t52/live

[13] http://www.broadcastify.com/listen/feed/219

[14] http://www.youtube.com/watch?v=ptTljYxuN_M

[15] The Republic, AZCentral.com, March 7, 2013, *Phoenix to shield police radio traffic.*

[16] Coloradoan.com, May 28, 2013, *Fort Collins police to silence public radio broadcast.*

smartphone apps. This was done to improve officer safety and to prevent exposure of citizens' private information. In this case, the media was allowed to use radios provided by the police to monitor dispatch channels only.

- **Allentown, Pennsylvania –** In 2012, the Allentown Pennsylvania Police Department[17] encrypted their radio system to "increase officer safety and enhance operational security". The Allentown Mayor believes this will prevent criminals from listening to sensitive transmissions with commercially available scanners and smart phone apps.

- **Fairfax County, Virginia –** In 2011, Fairfax County Police were dealing with home invasions and robberies targeting one ethnic group. After numerous incidents and calls from eyewitnesses, the police determined the perpetrators were deploying radio scanners to monitor and avoid responding police units.

  Proactive County communications officers were able to thwart these criminals quickly. They deployed encrypted radios within the Police and Sheriff Departments and distributed a communications plan to the police task force detailed to combat these activities. Within several days, the reaction teams intercepted the subjects in commission of a burglary involving breaking and entering.

- **Garden City, Kansas -** As reported in 2010[18], the Garden City Kansas Police Department decided to encrypt department radios for officer safety and criminal investigation purposes. Department officials stated that "The primary factor is the safety of the officers. Basically, it boils down to officers can now respond and coordinate efforts for certain incidents, and everybody doesn't hear it. Scanner traffic is available online now, and there are even applications for smart phones." Encrypting police traffic prevents criminals from using scanners to monitor police activity while committing crimes.

Some Key Issues

The decision regarding when and how to encrypt should include a requirement to resolve the important issues of encrypting radio traffic. A number of factors must be taken into consideration that may impact operability as well as interoperability.

- ***What to encrypt*** – Public safety agencies should review their jurisdictional legal requirements, operational environment, pertinent standard operating procedures, and communication vulnerabilities. If the intent is to prevent unauthorized persons from listening to or viewing the data, an agency may need to use encryption. As encryption protects sensitive information, it is not necessarily needed to protect routine

[17] The Express-Times, August 6, 2012, *Allentown Police Department switches to encrypted radios….*
[18] The Garden City Telegram, July 10, 2010, *Police Scanner Encryption Under Fire*.

information whose potential compromise does not adversely affect operations or endanger the public. Many agencies encrypt SWAT and surveillance operations, but do not encrypt day-to-day police activities. In many cases, emergency medical transmissions are often encrypted to protect patient privacy. Arguably though, emergency medical transmissions between the response vehicle and the medical facility can be hindered by encryption.

- ***How to Encrypt –*** The method of encryption is as important a decision as what to encrypt. The recommended encryption method is AES, as described in NIST publication FIPS 197. With a 256-bit key, AES is the P25 method of choice for encrypting sensitive information. It is believed that other currently available encryption methods do not offer the level of security required for public safety communications and can be easily decrypted.

- ***The impact on Interoperability -*** Another important factor to be considered when deciding whether to encrypt public safety radio systems is "how will encryption affect my ability to communicate within my agency, within my jurisdiction, with neighboring jurisdictions or regional/statewide systems, or with federal partners?" Consistent planning, deliberate system design, and close coordination with all stakeholders will help solve this potential interoperability issue. An example of how this potential problem can be overcome is provided by the Washington, D.C. National Capital Region (NCR). The NCR has created a Strategic Regional Encryption Plan with common zones that have shared encryption keys in both DES and AES to accommodate differences with existing capabilities. Regional zones in the radios allow for critical mutual aid responses to be on encrypted channels. Consideration must be given to the potential impact on interoperability when encryption is utilized in large scale events that include mutual aid agencies that do not typically respond together. Without effective planning, communication capabilities may be impacted.

- ***Public Information Access*** –The public information aspect of public safety communications can create conflicts with the operational needs of agencies. Some information needs to be protected to assure the integrity of ongoing investigations or incidents, where the release of such information would be detrimental to the safety of life and property. Public Information may be accessed through Public Information Officer (PIO) websites, social media feeds, or directly to the media. There are a number of legal issues regarding public access to public safety communications (non-broadcast) that need to be examined.

- ***General Cost Considerations*** - Cost is often cited as a primary reason many public safety agencies do not encrypt radio traffic. Although encryption does add cost to system procurement, it is not as much as has been suggested in some recent press releases and articles. There are a number of factors that influence the cost of encryption, including the method of encryption and how the encryption keys are maintained and distributed, as well as the cost to operate the cryptographic system and the size of the system. This additional cost can be difficult to justify in lean financial times, consequently a risk assessment should include the total added cost of encryption versus the impact of not encrypting sensitive information.

Essentially, a decision to not encrypt mission critical radio transmissions, despite the added cost, can have a negative impact on how effectively these operations are conducted. Most federal departments and agencies have thoroughly studied the impact and chosen a policy of protection. They have opted to encrypt most radio transmissions, especially mission critical operations such as law enforcement, defense, and homeland security.

Summary

The examples discussed provide real-world documentation regarding how encryption did or could have affected the outcome of public safety actions regarding criminal activity or the compromise of protected personal information. Some jurisdictions generally decide to encrypt in order to protect this information from the criminal element, and not to deny timely information regarding disasters or incidents from the public or the media.

In 2007, the National Institute of Justice[19] (NIJ) came to some key conclusions regarding voice encryption for radios including the fact that unencrypted public safety voice transmissions can be intercepted, abetting criminal activity, thwarting public safety efforts, and endangering the public and public safety personnel. Those conclusions apply equally today, but with added importance. Data transmissions on public safety radio systems are much more prevalent today and are increasingly used to transmit sensitive data on law enforcement activity, as well as personal and health privacy information. The protection of this information on radio systems is equally important to protecting voice transmissions, adding to the need for encryption more than ever.

With the development of broadband wireless systems, the need for encryption becomes more important in that the volume of information transmitted is increased[20], also increasing the potential exposure to unauthorized use. The design of the National Public Safety Broadband Network (NPSBN) by FirstNet should include the ability to protect sensitive public safety voice and data as well as provide for the management of the encryption system.

It is recommended that all the factors discussed here be thoroughly vetted and debated before reaching a decision regarding encryption for public safety radio systems. Federal agencies continue to recognize the importance of encrypting public safety radio communications and

[19] National Institute of Justice, *Voice Encryption for Radios*, NCJ 217103, Mar 2007.

[20] The greater the bandwidth, the greater the amount of information can be transmitted.

stress that encryption is vital to national security and mission integrity. State and local governments must consider 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, such as law enforcement sensitive information, personally identifiable information, and protected health information?**

APPENDIX A - Scenario-based Examples of how the lack of Encryption may Compromise Public Safety

There are a number of public safety events and scenarios where the encryption of critical communications may enhance response and mitigate loss or damage. These scenarios are generalized and are meant to illustrate potential reasons to consider encryption when developing public safety communications systems and strategies.

- **Active Shooter Incidents -** Over the years, law enforcement responses have evolved to meet the changing tactics of the active shooter threats. After-action reports for active shooter events regularly highlight the need for a coordinated response by law enforcement. In a rapidly evolving incident, accurate information must be provided to responders and they must coordinate their plans and movements to respond safely. First responders gain an advantage over adversaries when equipped with a voice radio system that allows them to communicate clearly during a response. However, the advantage is negated if the offender(s) are listening to the responding officers. Modern technology allows perpetrators to monitor police communications from a smart phone or an inexpensive scanner making it easier than ever before for unencrypted communications to be intercepted by suspects.

- **Urban Search and Rescue (USAR) Deployments -** Currently, Search and Rescue teams from FEMA and other agencies use radio systems that are encrypted on simplex, duplex and trunked talk-groups. When an event, such as a hurricane, or other major incident involving the deployment of these teams, they often manage, direct, and coordinate federal, State, and local assets responding to these incidents and must use the “lowest common denominator” to achieve interoperability. In many cases this is unencrypted communications.

  In the recent “Superstorm Sandy” event, numerous federal personnel were paired with State and Local personnel performing search and rescue missions throughout affected areas. In general, the federal personnel use encrypted radio systems but communicate with state/local personnel utilizing unencrypted radios, all potentially relaying or receiving the same information. These differences can easily cause confusion, and compromise sensitive information.

- **Training Scenario –** This scenario involves the adage that "you must train the way you fight". In some reported cases, law enforcement training exercises have exposed specific surveillance and tactical methods by being conducted in the clear, without encryption. By doing so, the methods that law enforcement officials use to apprehend criminals are exposed and can be anticipated by the criminal, thereby avoiding detection and apprehension. By using encryption in training exercises, as well as live activities, these procedures, tactics, and methods cannot be intercepted by anyone with a scanner.

- **Emergency Response to Major Incidents –** One of the concerns with not encrypting public safety radio traffic is the public, the media/press, and others will continue to react to a report where units (police, fire, EMS) are dispatched to the scene of a major incident (crash, fire, explosion, Hazmat, etc.), potentially causing a larger crowd than would otherwise be present and could cause control problems at the scene before the incident can be managed properly and before the public safety personnel can react to the emergency creating additional risk for media, citizens, victims, and responding officers.

- **Active Investigation and Surveillance Scenario –** In general, this scenario is where encryption can protect information involving ongoing investigations of the criminal element and possibly prevent crime or apprehend criminals in the act. These activities, in themselves, involve stealth and the need to protect all communications involved from public consumption. Without encryption, radio traffic that involves investigations, active surveillance/stakeout, or the information transmitted from a body wire to a surveillance vehicle can be intercepted by anyone with a scanner, potentially compromising the investigation. This also applies to the fire investigation process where fire department cause and origin specialists typically work with sensitive information and materials related to the case or incident. If an incident is of a larger magnitude and the investigation is of a sensitive nature, the need for encryption on specific channels/talkgroups that are assigned to fire investigation or fire marshal units is imperative.

- **EMS Scenario –** This scenario has two distinct sides to it. On one side, encryption of EMS/Medical traffic can create interoperability issues (as can any application of encryption). All links must be encrypted, including the link between the ambulance and the treatment facility, dispatch links, links between neighboring jurisdictions, etc. In these cases, encryption/key management can become difficult and complicated. Additionally, some jurisdictions use private or contract operated EMS/ambulance services, making it even more difficult to maintain and control communications security. This aspect has resulted in some jurisdictions forbidding encryption of EMS traffic.[21]

  On the other side, the lack of encryption of EMS traffic may compromise sensitive personal information possibly protected by the Privacy Act (see PII below), and could provide embarrassing information or information of a sensitive nature such as sexual

[21] The State of Minnesota Emergency Medical Services Communications Plan, January 26, 2012, recognizes the need to protect patient information, but requires that all EMS communications is to remain in the clear, stating that encryption causes confusion and does not promote interoperability.

assaults, child endangerment and abuse if transmitted without encryption for anyone to monitor.

- **Personally Identifiable Information (PII) Compromise –** Citizen PII is frequently broadcast in the clear, putting citizens at risk of identity theft, identification in the press, or by other unauthorized parties. This information may be exposed during traffic stops or in other routine, investigative, or emergency response incidents. This information exposes the transmitting agencies to a serious liability when the personally identifiable information (PII) is compromised in these scenarios and when the information transmitted is readily available to anyone with a scanner or Internet access.

- **Use of Scanners and Social Media -** The lack of encryption on voice channels that transmit law enforcement sensitive, sensitive medical information and personally identifiable information (PII) allows the public to listen and gather this information affording an opportunity to disseminate the information through various means including the Internet. "Hobbyists" currently scan, record, and rebroadcast Federal, State, and local public safety radio traffic and document it on a number of public web sites. Among the published examples in the Nation's Capital include Homeland Security counter surveillance missions, FBI aircraft activities, POTUS[22] movements, and 2013 Presidential inauguration surveillance information.[23]

  In addition, a number of jurisdictions have set up social media feeds to keep the public informed about public safety information, but some are reconsidering that decision and opting for encryption to protect ongoing investigations. During the recent Boston bombing incident, all law enforcement feeds were temporarily suspended at one point to protect law enforcement resources and their efforts during the manhunt underway in the Boston metropolitan area, testing the decision to make *all* information public immediately.

[22] President of the United States
[23] RadioReference.com, Scan DC archives

Appendix B – Report Contributors

The following Federal, State, and local public safety Departments and Agencies contributed to the creation and completion of this document. These contributions represent the combined opinions of recognized subject matter experts in the field of wireless encryption operations and technology.

- Connecticut Department of Emergency Services and Public Protection, Division of State Police
- Fairfax County (Virginia) Department of Information Technology, Radio Services Division
- Fairfax County (Virginia) Fire and Rescue
- Federal Bureau of Investigation, Operational Technology Division, Technical Programs Section, Radio Systems Development Unit
- FEMA, Disaster Emergency Communications Branch
- Florida Department of Highway Safety and Motor Vehicles
- Lake County (Florida) Department of Public Safety
- Metropolitan Washington Airports Authority, Wireless and Radio Systems Department
- Missouri Department of Public Safety, Missouri Interoperability Center
- Montgomery County (Maryland) Police Department
- Montana Department of Justice, Highway Patrol Division
- National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division
- Orange County (California) Sheriff’s Department, Radio-Microwave Unit
- Phoenix (AZ) Police Department
- Portland (OR) Public Safety Radio Communications Revitalization Program
- State of South Carolina, Office of the CIO

- Texas Department of Public Safety
- Treasury Inspector General for Tax Administration, Technical and Firearms Division
- U. S. Bureau of Reclamation
- U.S. Capital Police, Communications Division
- U.S. Coast Guard
- U.S. Department of Justice, Wireless Management Office
- U.S. Department of Homeland Security, Customs and Border Protection, National Law Enforcement Communications Center
- U.S. Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations
- U.S. Department of Homeland Security, Office of Coordination and Planning
- U.S. Marine Corps, MCAS Yuma, Communications Data Electronics Department
- Washington D.C. Fire and Emergency Services Department
- Wyoming Public Safety Communications Commission

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, and 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 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.

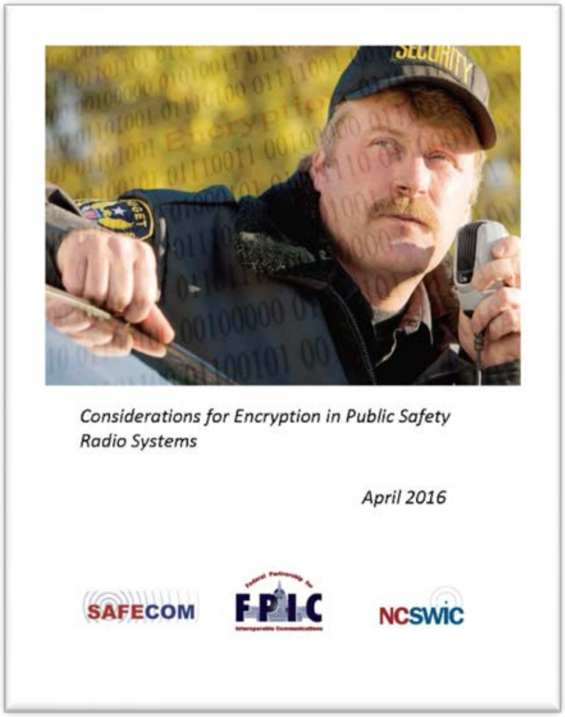
[1] "In the clear" transmissions are unencrypted radio signals that are open to reception and listening by anyone with a receiver.

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 this 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.



Considerations for Encryption in Public Safety Radio Systems

April 2016

SAFECOM FPIC NCSWIC

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 airwaves. 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 use encryption 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 different 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 assist public safety users as they embark on a process to assess their need for encryption.

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

September 2016

SAFECOM

Federal Partnership for FPIC Interoperable Communications

NCSWIC

Contents

Preface

As the public safety user community has continued to recognize the importance of protecting sensitive information, the interest in encrypted communications has steadily increased. This document specifically addresses the complex issues of key management and the importance of common procedures.   As was the case for two previously published documents addressing encrypted communications noted in the *Introduction*, the incentive for this document came from a request from the state and local public safety community, particularly the non-federal members of the Federal Partnership for Interoperable Communications (FPIC) Security Working Group (SWG) to provide guidelines and best practices to be considered when implementing encrypted communications. It is essential that the design and operation of mission critical radio systems enable voice and data communications that are protected from unauthorized reception as well as provide communications interoperability as required.

There were a significant number of public safety officials and systems administrators that recognized the importance of encryption and the need to address common key management methods. This document begins to outline how key management can be approached in a standard way so that the coordination of key parameters can help to enhance encrypted interoperability at all levels of government. In addition, a *Fact Sheet* has been developed to accompany this document that provides a high-level summary of the key facts, issues, and recommendations for the encryption of public safety radio systems at all levels of government.

This report is a result of an extended effort by the Federal Partnership for Interoperable Communications (FPIC) Security Working Group[1] and other contributing individuals, agencies, and organizations outlined in Appendix C. In addition, the FPIC wishes to acknowledge the valuable input of the following groups and organizations: Department of Homeland Security OneDHS[2], SAFECOM EC[3], NCSWIC EC,[4] SAFECOM-NCSWIC Technology Policy Committee, and the DHS Southwest Border Communications Working Group[5]. It is important to note that there are significant governance, policy, and training implications that must be considered with the use of encryption.

[1] The FPIC is recognized as a technical advisory group to SAFECOM and the ECPC.

[2] OneDHS worked to coordinate and integrate communications activity within DHS.

[3] SAFECOM was formed in 2001 after the terrorist attacks of September 11, 2001 as part of the Presidential E-Government Initiative to improve public safety interoperability, allowing emergency responders to communicate effectively before, during, and after emergencies and disasters

[4] NCSWIC assists state and territory interoperability coordinators with promoting the critical importance of interoperable communications and the sharing of best practices to ensure the highest level of interoperable communications across the nation.

[5] SWBCWG serves as a forum for F/S/L/T agencies in Arizona, California, New Mexico, and Texas to share information on common communications issues; collaborate on existing and planned activities; and, facilitate federal involvement in multi-agency projects within the Southwest Border Region.

1. Executive Summary

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 communications.

Successful encrypted interoperability depends largely upon improved coordination between agencies that need to interoperate. It is also enhanced when all agencies understand how the use and coordination of key management parameters can affect their ability to interoperate. It is vital that agencies implement encryption and key management in a consistent manner and in collaboration with other public safety agencies.

The *Best Practices* discussed in this document provide an understanding of how basic key management parameters are related in Project 25 land mobile radio (P25 LMR)[6] systems. In addition, the document addresses improved coordination of these elements, and the use of standards-based encryption can enhance encrypted interoperability while minimizing the risk of compromising sensitive information. Examples of these *Best Practices* are listed below.

- **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.
- **Standards-based Encryption** – Use P25 standard AES-256[7] security solution to protect against compromise.
- **Crypto Period Considerations** – Use defined crypto periods to mitigate risk.
- **Communications Planning** – Develop Communications Plans that incorporate encryption requirements.
- **Education and Training** – Develop appropriate training for system personnel to improve effectiveness.
- **Exercise and Testing** - Develop and execute regular communications exercises and testing to maintain effectiveness.
- **Outreach** – Collaborate with experts to ensure effective encryption implementation.

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

[7] FIPS 197, *Advanced Encryption Standard*, Nov 2001

Although these best practices are considered important in developing an environment where encrypted interoperability is realizable, significant additional planning and coordination must be accomplished to enable progress on a national scale. Leadership in developing more detailed encryption guidelines and support for further education and outreach is also needed. These best practices are governed by the same guiding principles of the Interoperability Continuum[8] in that they are based on the goal of interoperability by effective leadership, planning, and collaboration among public safety agencies.

2. Introduction and Background

Reliable, secure encryption techniques applied to public safety radio systems can provide the safeguard needed to ensure the protection of sensitive information from unauthorized use. Once that decision is made, the encryption equipment has been installed, and the system administrator is ready to employ encryption on parts or all of the radio system, key management becomes the primary task. What comes next is the realization that radio encryption, when properly used, requires a degree of maintenance in setting up the initial encryption scheme, programming radios, providing the initial encryption key(s) to the system and radios, and developing a key management protocol to ensure that security is maintained.

This document supplements two other documents addressing encryption in public safety land mobile radio systems. In February 2016, SAFECOM, NCSWIC and FPIC jointly published *Guidelines for Encryption in Land Mobile Radio Systems*, which outlined and discussed the encryption methods that can be used to protect sensitive information for public safety radio systems. Previously, in November 2014, the FPIC developed *Considerations for Encryption in Public Safety Radio Systems*, which provided real-world examples of why encryption is needed and discussed issues involved in making that decision, and is pending publication as a joint SAFECOM/NCSWIC/FPIC document[9]. Together, these documents provide public safety agencies with some important information for deploying encryption in land mobile radio systems. Hopefully, these reports will allow agencies to develop strategies for justifying the additional cost and complexity that encryption adds to system planning, architecture, and operation.

As state, local, and tribal public safety agencies began to implement encryption systems throughout the Nation, the users began to realize that additional guidance and education would be beneficial to ensure that encryption was applied in a reliable manner and that common key management methodologies are available to provide consistent practices among Federal, state, local, and tribal public safety agencies. Although the emerging Project 25 Digital Standards provide enhanced capabilities and interoperability, the basic methods and protocols for encryption have been developed and tested by Federal agencies over the past several decades and have proved reliable and secure.

[8] http://www.dhs.gov/publication/commonly-accessed-documents-safecom
[9] www.dhs.gov/technology

Based on the knowledge gained through years of use and applied throughout the Federal Government on a daily basis, the FPIC[10] Security Working Group (SWG) has been developing strategies for key management that can be applied at all levels of government to assure compliance with the standards[11] that govern how encryption in public safety grade Project 25 (P25) land mobile radio systems works. Additionally, as encrypted interoperability becomes more common among first responders, common procedures will be needed to ensure that systems from different jurisdictions and different manufacturers remain protected and interoperable.

3. Purpose

The purpose of this document is to highlight those elements and best practices of key management that are needed to allow encrypted operability as well as interoperability. The importance and relationship of the elements of key management will be addressed. Fundamentally, the intent of this document is to simplify the complex process of encryption and key management so that *only the essential elements or parameters that are needed for operability and interoperability* are described. The primary goal is to identify Best Practices[12] for the basic aspects of key management, so that encrypted interoperability is possible and manageable among public safety agencies at all levels of government.

The details of how encryption works in a P25 system is contained in the ANSI/TIA 102 Series of Standards[13], and key management guidance is provided in by the National Institute of Standards and Technology (NIST) SP 800-57 series of publications.[14] The standards describe how encryption enables these systems to maintain a robust security profile that protects sensitive information from compromise. This document will address how and why certain encryption parameters are crucial to maintaining a well-functioning encryption system that will assure security and enable interoperability in the encrypted mode.

4. Key Management Overview

In general, key management is the process for the creation (generation), distribution, use, archiving, and destruction of cryptographic keys in a P25 land mobile radio system. It is a vital

[10] The FPIC serves as a coordination and advisory body to address technical and operational wireless issues relative to interoperability within the public safety emergency communications community. The FPIC serves as an interface between the federal, state, tribal, and local agencies. It includes more than 200 federal, state, local, and tribal public safety representatives from over 45 Federal agencies, as well as representatives from State, tribal and local entities.

[11] TIA standards and NIST standards listed in Appendix C

[12] A *Best Practice* is commonly defined as a methodology developed through investigation and experience that has proven reliable and effective.

[13] The published American National Standards Institute/Telecommunications Industry Association ANSI/TIA-102 Standards are available at https://Global.ihs.com.

[14] NIST SP-800-57, *Recommendation for Key Management, Parts 1-3*

part of maintaining a secure operating environment for any public safety radio system. This document will not include a detailed discussion or description of this relationship or details of all the components of key management. Instead, a description of how certain parameters of key management affect interoperability and the importance of maintaining good key management procedures will be included. Without proper and consistently applied key management techniques and protocols, system administrators at different agencies and various levels of government may find it difficult to assure security throughout their system. If common protocols and best practices are applied across all levels of government, encrypted interoperability becomes less onerous.

The P25 Security Services Overview document [15] addresses the need for agencies to develop a key management procedure or doctrine within each organization. The P25 standards do not provide a key management standard. The only elements of key management specifically addressed by the standard are key distribution, entry and use within system elements. NIST provides specific guidelines for establishing a key management program for the proper management of cryptographic keys, including *best practices, general organization and management requirements, and implementation specific key management guidance.* Additionally, the resources listed in Appendix B can provide further guidance in developing key management processes and implementing encryption systems, as they represent a significant source of knowledge and experience in the subject.

Each of the aspects of key management plays an important role in maintaining an effective key management process within an agency. Although simplified in this document, cryptography in P25 land mobile radio systems and key management are complex processes that must be well understood and coordinated to be effective.

Key Generation

The two basic types of keys referred to in this document are the Traffic Encryption Key (TEK)[16] and the Key Encryption Key (KEK). The TEK is the primary key that encrypts voice and data transmissions. The KEK encrypts one or more TEKs (or other KEKs) and is used to identify/authenticate a group of TEKs. Another type of key is the Unique Key Encryption Key (UKEK), a unique KEK that is common to only an individual subscriber unit (SU) or Key Fill Device (KFD) and the Key Management Facility (KMF) and is used to create a secure link during initialization with an individual unit within the KMF's management. These keys can be generated by various key generators, both manually and automatically. The generation of keys is normally accomplished within the agency that manages the encrypted radio system with one of various key generation methods. Once generated, keys can be loaded or distributed through various methods discussed below. The importance to encrypted interoperability is that keys need to be coordinated and shared with other agencies if interoperability is to be realized.

[15] TIA-102.AAAB-A, *Project 25 Digital Land Mobile Radio – Security Services Overview*, Jan 2005

[16] The TEK is a unique hexadecimal key used to encrypt and decrypt voice and data traffic. The length of the TEK depends on the algorithm used.

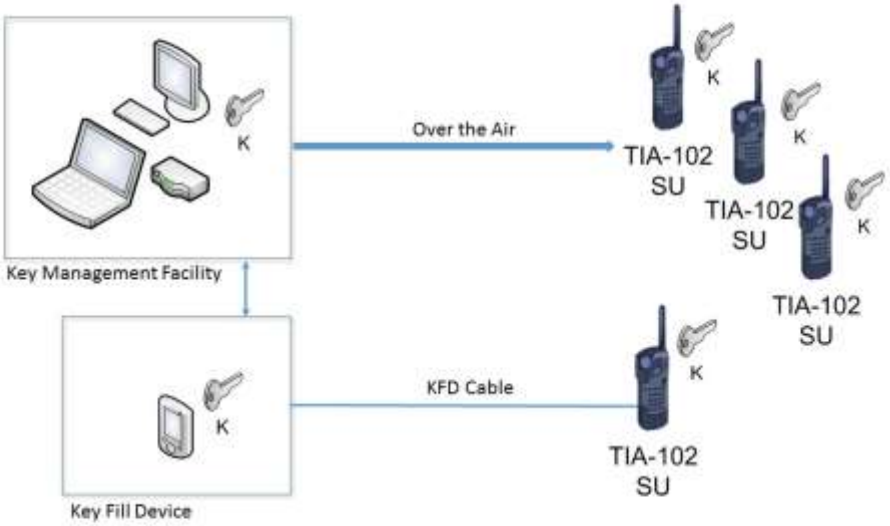
Obviously, without the proper key (and other important parameters identified in Section 5), transmissions cannot be decrypted.

Key Distribution and Use

This is where encrypted interoperability is proven. The only way for jurisdictions to interoperate in the encrypted mode is to share common keys and coordinate the distribution of those keys. The preparation for ensuring encrypted interoperability within an agency, among agencies of neighboring jurisdictions, and on a national level requires a significant amount of planning and cooperation.

The distribution of keys for P25 radios can be accomplished using a KFD for loading keys into subscriber units manually or a KMF for loading keys into subscriber units using OTAR (Over-the-Air-Rekeying). These devices also provide for the management of the key system. Figure 1 below shows that relationship. KFDs can also be programmed or managed by KMFs so that field personnel can load keys in remote areas or in special circumstances. A KMF provides for centralized key management and can include a web-based interface for IP connectivity. A KMF allows for remote inhibit/permit of radios, where a KFD must "touch" each radio for loading keys. The parameter *K* in Figure 1 (and wherever it appears) represents the key variable, hereafter referred to as the TEK, which is used to encrypt the transmission.

Figure 1: KMF, KFD, and Subscriber Unit Interfaces



Key Archiving and Destruction

If keys or keying material needs to be recoverable, for whatever reason, then it needs to be archived and maintained by a trusted party. When it is no longer needed, all copies of the keying material should be destroyed with a method that removes all traces of the keying material to ensure it cannot be recovered by either physical or electronic means[17]. In general, these elements must be addressed when developing common key management policy and procedures for interoperability among multiple agencies.

5. Importance of Coordinated Key Management

As stated, key management is the process for the administration of cryptographic keys in a LMR system. It consists of a complex set of relationships between the P25 Common Air Interface (CAI), the Encryption Protocol, and the Key Management Protocols described in the P25 TIA-102 Security Services series of standards and elaborated upon in the NIST SP-800-57 publications. It is important to note that a key management policy in a department or agency should address the key management process that is appropriate for each user organization.

Since the practice of encryption and key management varies significantly between public safety agencies, it is essential that these policies/procedures be managed in a consistent way among agencies implementing encryption. In addition, close coordination of these policies and practices among users, especially among joint task forces and neighboring jurisdictions, is essential so that interoperability can be achieved in the encrypted mode at incidents or joint operations. Without a coordinated approach, where agencies have established common encryption groups with shared keys, encrypted interoperability among agencies would experience significant challenges.

Elements of Encrypted Interoperability

There are many complex elements of key management that must be addressed to ensure an effective and secure encrypted radio system. Encrypted interoperability, however, depends on how well jurisdictions that need to interoperate coordinate their protocols and methods for key management. To ensure dependable results, agencies should ensure those policies are consistent with National Guidelines/Best Practices being developed within the FPIC SWG.

Fundamentally, LMR encryption works between two or more radio units or consoles. Voice or data enters one radio, is encrypted through a process that involves a number of parameters, including the appropriate encryption algorithm and TEK. All elements in this process must be synchronized and aligned (common) for the encryption/decryption process to work properly. If the receiving radio contains the proper parameters or identifiers, then the received traffic is decrypted. The alignment of these parameters should be a given for an agency that operates encrypted radios only within its own radio system. The agencies control each of the parameters, which are assigned when programming the subscriber units within a system. It becomes complicated when an agency must coordinate these parameters with other agencies or among a number of agencies, such as a task force.

These critical parameters or identifiers include:

- **The Key ID (KID**) - Provides a unique address to identify a Traffic Encryption Key. The KID is a 16-bit identifier that has a reserve value of hexadecimal $0000 for unencrypted traffic and can be used for single key radios. The P25 Block Encryption Protocol, TIA-102.AAAD-B, specifies hexadecimal[18] $0000 as a reserve value and is used as a default KID for equipment that is not capable of multi-key operation. It is strongly recommended that this reserve value not be used in single key radios, as this will cause the radio to ignore any messages originated from multi-key devices that use non-default key values.

- **Traffic Encryption Key (TEK)** - The Key Variable, a unique hexadecimal key used to encrypt and decrypt voice and data traffic.

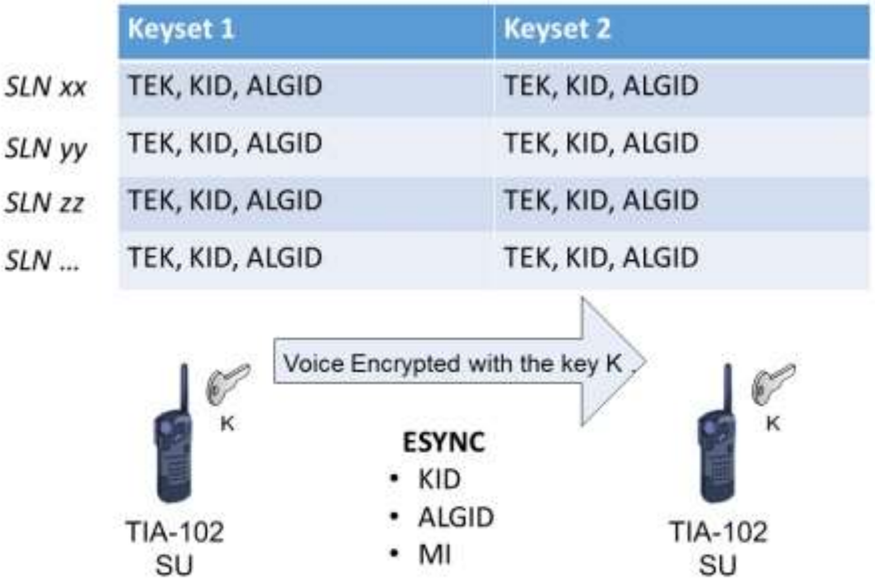
- **The Storage Location Number (SLN),** a common term to refer to an encryption key slot in a subscriber unit (also referred to as the CKR[19]). In cases when the key is strapped to a specific talk group, the SLN can be used to designate the encrypted talk group.

- **The Algorithm ID (ALGID)** - an indicator of the type of encryption used. The ALGID is a static hexadecimal value established based on what type of encryption is present. Unencrypted has a reserved value of $80, DES is $81, AES128 is $85, and AES256 is $84.

One or more Keys are categorized by a KID and the appropriate ALGID that identifies the encryption algorithm used, and are stored in the SLN in the radio. The SLN is used to designate a collection of keys (multiple encryption keys within a radio) that may be used for an encrypted operation or target, and can be used to designate a cryptographic talk group. The combination of the Key ID and the Algorithm ID uniquely identifies a key within the KMF/KFD or subscriber unit. The KID and the TEK must match for the process to work properly and for the receiving radios to decrypt transmissions. Multiple encryption keys can be stored in radio equipment conforming to the standard. In order to identify the keys, they are stored with an associated label, the KID.

[18] The “$” is an indicator that the value is hexadecimal and is not programmed in the software.
[19] CKR or Common Key Reference is a term used in Motorola programming software.

Figure 2: Essential Indicators for Encrypted Interoperability



	Keyset 1	Keyset 2
SLN xx	TEK, KID, ALGID	TEK, KID, ALGID
SLN yy	TEK, KID, ALGID	TEK, KID, ALGID
SLN zz	TEK, KID, ALGID	TEK, KID, ALGID
SLN ...	TEK, KID, ALGID	TEK, KID, ALGID

Figure 2 above illustrates, in basic terms, the relationship of the parameters or indicators needed for this process to work effectively. Encryption synchronization (ESYNC) represents the elements required for the transmitter (TX) and receiver (RX) to synchronize transmission, including the Message Indicator (MI) that provides the basic synchronization information, but does not affect the actual encryption process. The SLN is a location programmed in the radio that contains the position of the keyset(s). The KID, the ALGID and the TEK allow the RX to decrypt the transmission. The table within the figure shows what is stored in the subscriber unit for encryption purposes. Each SLN (0 through 4095) contains the key indicators that are needed for encryption to work: the key, the KID, and the ALGID. This illustration shows a multi-key configuration where the current keyset and the future keyset are stored in a particular SLN.

In simplified terms, encrypted interoperability hinges on the coordination of all of these parameters among those agencies needing to interoperate. Encrypted interoperability depends not only on the coordination of these parameters, but on how well jurisdictions who need to interoperate coordinate their protocols and methods for key management. These agencies should ensure that plans and policies are developed to include their own encryption requirements as well as those necessary to operate with other jurisdictions.

The Current Environment

In general, key management is left to the agency that manages the land mobile radio system. It is normally accomplished at a local agency level but is sometimes coordinated on a broader level, such as county, region, or state. However, many public safety agencies who have implemented encryption have limited experience in key management and could benefit greatly from learning about how their current key management policies may adversely affect the vulnerability of the information they transmit. As an example, they may use the same SLN for all radios, when a more organized use of the SLN is to treat it as a type of encrypted talk group to segment user groups for certain purposes, such as Task Force, Incident Response, SWAT[20], or investigations. As discussed below, some SLNs can be reserved on a National basis for use in creating regional and National response groups for encrypted communications.

In addition, some agencies use static keys and crypto periods for sensitive operations, meaning the TEK is *never* changed. If the key is compromised in whatever manner, any information on the encrypted channel is potentially compromised. Currently, there is a mix of agencies who are well informed on key management and those who are new to the game and need help in understanding its complexities.

Federal agencies differ from state and local agencies in that they have national missions and must deal with managing encryption and key management in a more centralized way and on a broader scale. Much of federal land mobile radio assets are encrypted, and many federal departments and agencies provide for their own key management. A major force in the management of federal land mobile radio systems and provider of key management services to many federal as well as state and local public safety agencies is the National Law Enforcement Communications Center (NLECC) in Orlando, Florida. The NLECC is a Department of Homeland Security/Customs and Border Protection facility whose primary mission is to manage all aspects of DHS/CBP land mobile communications, but has gained expertise in providing key management services to many other agencies at all levels of government. The use of the NLECC to generate and assign Keysets (KID, Key, ALGID) for agencies at all levels of government assures that these parameters are unique and will not conflict with other systems that also use NLECC services. Using a national coordination entity helps to ensure a more uniform approach to key management.

For state and local agencies, the Statewide Interoperability Coordinator (SWIC)[21] can provide the basic point of contact within each state and territory for information on encryption and how to best coordinate encrypted interoperability with partner agencies. They have the knowledge regarding the local environment and know the local encryption experts. They also are members of the National Council of Statewide Interoperability Coordinators (NCSWIC)[22] and can act as a coordinator for coordinating key management with other state and local agencies in the region and assistance from the NLECC as well as with other national organizations and federal agencies.

In general, public safety agencies have varying requirements for encryption and deploy a number of different techniques for managing their encryption. They range from *no encryption*

[20] SWAT (Special Weapons and Tactics) – specialized law enforcement units that use specialized equipment and tactics.

[21] The SWIC is the primary coordinator in each State and territory for the operation of the state's interoperability efforts.

[22] NCSWIC (composed of SWICs) assists state and territory interoperability coordinators with promoting the critical importance of interoperable communications.

to fully-compliant P25 *AES encryption.* Many state and local agencies limit the use of encryption to SWAT, Investigations, or other operations that require protection of sensitive transmissions. Others may use non-standard privacy techniques such as RC4[23], which will not provide the degree of protection that P25 AES provides, is not recommended for transmission of sensitive or mission critical information, and is not approved for federal government use.

For those agencies who do employ P25 standard encryption (DES [24]or AES), key management is usually accomplished in one of two primary ways:

- Use of a Key Fill Device (KFD) which is programmed with the KID and the TEK and is manually loaded into each radio. The key management is accomplished locally, and key changes must be accomplished manually.
- Use of a Key Management Facility (KMF) that provides Over-the-Air-Rekeying capability. The KMF also can be used to manage the configuration of Key Fill Devices.

Those systems that do not have an OTAR capability must use a Key Fill Device or other method for key management. This mix of methods for loading keys into radios can cause conflicts in that all keys are not generated by the same source and may not be coordinated or shared with other jurisdictions.

In addition, the use of the SLN is sometimes random and can cause conflicts when SLNs are duplicated in the same or neighboring jurisdiction. The coordination of SLN assignments is one of the key factors to achieve encrypted interoperability and avoid conflicts. Ideally, the coordination of SLN assignments on a National or regional basis can be effective in avoiding conflicts when attempting to interoperate with other jurisdictions.

How can we achieve Encrypted Interoperability?

As difficult as regular interoperability has been to achieve, it seems achieving encrypted interoperability is beyond reason to some. In fact, encrypted interoperability presents the same roadblocks as unencrypted interoperability: dissimilar frequency bands, technology differences, policy and procedural/coordination issues, and many other factors. In addition, encryption brings further complexities to the table. The coordination of parameters, such as SLN and encryption keys, the methods and policies for general key management, the crypto period, and common naming conventions, can all contribute to the lack of interoperability.

Encrypted interoperability requires a number of factors to be coordinated among agencies that require interoperability. Primarily, the desire to interoperate and to coordinate with one another on a National or Regional level is a key driver. The Interoperability Continuum relies on

[23] RC4 is a stream cipher. It is initialized with a variable length key, typically between 40 and 256 bits, using the *keyscheduling* algorithm (KSA). The key stream of bits is generated using a pseudo-random generation algorithm (PRGA).

[24] Although DES is no longer approved for federal agency use, it remains a part of some installations, awaiting replacement.

Governance and Standard Operating Procedures to form the basis of interoperability. Encrypted interoperability also relies on these basic principles and suggests that the adoption of common key management policies and procedures can form the basis for improved encrypted interoperability.

Essentially, this type of interoperability requires the desire to interoperate; the knowledge and understanding of key management; coordination, planning, implementation, and cooperation between agencies; and a standards-based key management system. In addition to the training received by the vendor, there is a network of telecommunications managers and technicians who have years of experience in the details of key management and can be relied upon to help implement an effective encrypted P25 land mobile radio system. Those resources are listed in Appendix B. They include the National Law Enforcement Communications Center (NLECC), the NCSWIC, and the FPIC Security Working Group.

Encrypted interoperability depends not only on cooperation, but also on coordination of the parameters discussed above; the SLN, the KID, the ALGID, and the TEK. Since there are so many combinations of these parameters that must align before encrypted transmissions can be decrypted, prior coordination among all agencies that need to communicate is essential. Ideally, a common set of SLNs designated for specific purposes (general interoperability, tactical, law enforcement, Fire, etc.) must be defined and recognized on a National basis, so that they can be pre-programmed into radio systems prior to events in order to avoid unnecessary conflicts. As a start to realizing encrypted interoperability on a broader scale, the FPIC has developed Appendix A, *National Reserved SLN Table* in much the same way the FCC and NTIA have identified National I/O channels[25]. These SLNs (1-20) are designated based on encryption type, purpose, and recommended crypto period, and should be avoided in the assignment of local SLNs during programming.

6. Recommended Best Practices for Encrypted Interoperability

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 their encryption system to meet their own unique needs while also supporting common encrypted interoperable channels in their area of operations.

The FPIC Security Working Group has collaborated with LMR security experts at the federal, state, and local government level to examine the methods and procedures that lead to effective

[25] FCC Public Safety and Homeland Security Bureau at http://transition.fcc.gov/pshs/techtopics/techtopics12.html and NTIA Rules at 4.3.16

encrypted interoperability. Primary Best Practices that lead to effective use of encryption include:

Key Management Organization

Ensure the proper organization, implementation planning, and testing of the key management process prior to final implementation. This includes organizational key structure for various disciplinary needs (LE, Fire, EMS, SWAT, etc.) and assignment of the SLN to accommodate those needs. As a start, establish an effective, interoperable key management procedure within your agency. Effective key management includes day-to-day operation as well as planning for contingencies. Planning should include shared keys for events, emergency response, and contingencies. Think of who you will need to interoperate with before the event. The P25 TIA-102.AAAB-A Security Services Overview Standard governs how various aspects of security requirements and key management are specified for P25 LMR systems.

Key Generation and Distribution

Adopt the standard generation and distribution of SLN, KID, Keys, and other parameters that is defined in the P25 TIA series of standards listed in Appendix D. The P25 TIA-102.BAKA KMF-to-KMF Interface Standard presents a generalized concept of operations for managing interoperability keys. A standard for the KMF-to-KFD Interface is under development consistent with current standards addressing the KMF-to-KMF Interface and the KFD Interface Protocol. In that concept, the interoperability of key sharing, both inside and outside an agency, is determined by local agency policy, and ideally should be coordinated among neighboring jurisdictions. The NLECC has helped many agencies at all levels of government in providing keys for both P25 AES and P25 DES systems, and the SWIC is an ideal coordinator for developing key sharing plans.

National SLN Assignment Plan

Promote the use of the Storage Location Number in a common configuration to enhance National encrypted interoperability. The FPIC has developed a plan to reserve SLNs 1-20 to be used for National Interoperability. The Plan, shown in Appendix A, lists reserved values of the SLN and designates them for National, regional, local, task force, and incident response for various public safety disciplines. By adopting this plan, public safety agencies at all levels can begin to coordinate encrypted interoperability plans while minimizing SLN and Key conflicts with neighboring jurisdictions or within Task Force situations.

Standards-Based Encryption

Encourage the use of the P25 security solution using the Advanced Encryption Standard (AES-256). The P25 standard also defines processes and procedures for key management. If interoperability is required with federal agencies, an AES capable radio system is strongly recommended. Although DES is still in use, support for DES will eventually be concluded. The use of multi-key radios is highly recommended to enable the deployment of OTAR for current or future use. The use of non-standard encryption is inconsistent with NIST recommendations and cannot provide protection from compromise. A claim that a particular non-standard encryption method is capable of providing adequate security is arguable. Algorithms such as RC4 and other ciphers are *not* P25 standards and should not be used.[26]

Crypto Period Considerations

Encourage the use of a key with a defined crypto period to mitigate the risk of compromise (see NIST SP 800-57). Many agencies use a monthly crypto period and can change keys immediately if a key has been compromised. Static crypto periods should be avoided as much as possible. Although not discussed in this document, the understanding of how the crypto period affects the effectiveness of the key management process is as equally important as other elements of key management.

Communications Planning

Ensure that communications plans incorporate encryption requirements. Make encryption part of the Incident Radio Communications Plan (ICS 205) as well as multi-jurisdictional, and multi-discipline plans.

Education and Training

Promote the development and dissemination of accurate information regarding effective key management so that all public safety agencies can develop policies that allow for interoperability at regional, state, and national levels. Train LMR managers, technicians, Communications Unit Leader (COML), and Communications Unit (COMU) personnel in encryption interoperability methods and key management.

Exercise and Testing

Develop and execute regular exercises and testing to maintain effectiveness in encrypted operations. Testing and analysis of encryption and key management procedures and equipment is vital to maintaining the technology and ensuring availability when needed. Exercises within an agency and among jurisdictions that need to interoperate help to resolve common problems and guarantee encrypted communications interoperability during joint operations or incident response.

Outreach

Collaborate with the experts. Most importantly, talk to someone who has done this before. Learn from others' mistakes. Benefit from the knowledge of others with years of experience. If you have any questions regarding how to best implement encryption in your P25 LMR system, do not hesitate to ***Ask for Help!***

[26] SAFECOM/NCSWIC/FPIC, *Guidelines for Encryption in Land Mobile Radio Systems*, February 8, 2016. www.dhs.gov/technology

Appendix A: National Reserved SLN Table (6/19/15)

SLN	Algorithm	Use	SLN Name	Crypto Period (Annual key changes are completed on the first working Monday of October)
1	DES	Public Safety Interoperable	ALL IO D	Annual
2	DES	Federal Interoperable	FED IO D	Annual
3	AES	Public Safety Interoperable	ALL IO A	Annual
4	AES	Federal Interoperable	FED IO A	Annual
5	DES	National Law Enforcement State and Local Interoperable DES	NLE IO D	Static
6	AES	National Law Enforcement State and Local Interoperable AES	NLE IO A	Static
7	AES	US – Canadian Fed Law Enforcement Interoperability	FED CAN	Static
8	AES	US – Canadian PS Interoperability	USCAN PS	Static
9	DES	National Tactical Event	NTAC D	Single Event Use – Not to exceed 30 Days
10	AES	National Tactical Event	NTAC A	Single Event Use – Not to exceed 30 Days
11	DES	Multiple Public Safety Disciplines	PS IO D	Static
12	AES	Multiple Public Safety Disciplines	PS IO A	Static
13	DES	National Fire/EMS/Rescue	NFER D	Static
14	AES	National Fire/EMS/Rescue	NFER A	Static
15	DES	National Task Force Operations	FED TF D	One time use as needed for Special OPS
16	AES	National Task Force Operations	FED TF A	One time use as needed for Special OPS
17	DES	National Law Enforcement Task Force (one time only operation)	NLE TF D	One time use as needed for Special OPS
18	AES	National Law Enforcement Task Force (one time only operation)	NLE TF A	One time use as needed for Special OPS
19	AES	Federal – International Law Enforcement Interoperability	FED INTL	When needed by operational requirement
20	AES	Public Safety – International Law Enforcement Interoperability	PS INTL	When needed by operational requirement

Appendix B: 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:

1. The National Law Enforcement Communications Center (NLECC):
   Email: nlecc-wsoc@cbp.dhs.gov

2. Statewide Interoperability Coordinator (SWIC) for each of the 56 states and territories:
   see http://www.dhs.gov/safecom/contact-information

3. The Federal Partnership for Interoperable Communications Security Working Group:
   Email: FPIC@hq.dhs.gov

Appendix C: Report Contributors

The following federal, State, and local public safety Departments and Agencies contributed to the creation and completion of this document. These contributions represent the combined opinions of recognized subject matter experts in the field of encryption and key management.

- Connecticut Department of Emergency Services and Public Protection, Division of Statewide Emergency Telecommunications
- Fairfax County (Virginia) Department of Information Technology, Radio Services Division
- Federal Bureau of Investigation, Operational Technology Division, Technical Programs Section, Radio Systems Development Unit
- Montana Department of Justice, Highway Patrol Division
- Orange County (California) Sheriff's Department
- Phoenix (Arizona) Police Department
- State of South Carolina, Office of the CIO
- Texas Department of Public Safety
- Treasury Inspector General for Tax Administration, Technical and Firearms Support Division
- U.S. Coast Guard Headquarters
- U.S. Department of Homeland Security, Customs and Border Protection, National Law Enforcement Communications Center
- U.S. Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations
- U.S. Marine Corps, MCAS Yuma, Communications Data Electronics Department
- Wyoming Public Safety Communications Commission

Appendix D: References [27]

- FIPS 197, Federal Information Processing Standards Publication 197, *Specification for the Advanced Encryption Standard*, November 2001

- FIPS 140-2, Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, December 2002

- NIST SP-800-57, National Institute of Standards and Technology Special Publication SP-800-57, *Recommendation for Key Management, Parts 1-3*

- NIST SP 800-152, National Institute of Standards and Technology Special Publication SP-800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems*

- TIA-102.AAAB-A, *Project 25 Security Services Overview*, January 2005

- TIA-102.AAAB-A-1, *Project 25 Security Services Overview Addendum 1 – Key Management Architecture,* September 2014

- TIA-102.AACA-A, *Project 25 Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures*, September 2014

- TIA-102.AACE-A, *Project 25 Digital Land Mobile Radio Link Layer Authentication*, April 2011

- TIA-102.BAKA, *Project 25 KMF to KMF Interface*, April 2012

- TIA-102.AAAD-B, *Project 25 Block Encryption Protocol*, December 2015

- TIA/EIA-102.AACA-A, *Project 25 Digital Radio Over-The-Air Rekeying (OTAR) Protocol*, September 2014

- TIA-102.AACD-A, *Project 25 Digital Land Mobile Radio-Key Fill Device (KFD) Interface Protocol*, September 2014

[27] To access the latest versions of the information listed, check the reference sources at http://www.NIST.GOV and http://www.GLOBAL.IHS.COM

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 communications 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 agencies with interoperability needs.

THE REPORT

The Federal Partnership for Interoperable Communications (FPIC), in coordination with 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.

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

May 2016

[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 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 encryption key management, making encrypted interoperability 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[3] 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 system 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] http://www.dhs.gov/publication/commonly-accessed-documents-safecom

The T-Band Giveback

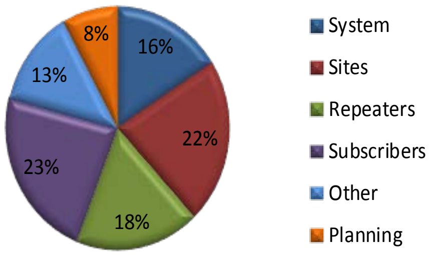
Implications for the Public Safety Community

The Middle Class Tax Relief and Job Creation Act of 2012 (Public Law 112-96[1]) requires the Federal Communications Commission (FCC) to recover and auction T-Band spectrum[2], currently in use by public safety agencies, for commerical use by February 2021. Additionally, the Act requires the FCC to clear public safety operations from this portion of the band within two years of auction close (i.e., early 2023). The ultra-high frequency (UHF) spectrum between 470–512 megahertz (MHz)—also known as the "T-Band"—supplies a significant complement of channels to support public safety operations and regional interoperability in 11 of the largest U.S. metropolitan areas[3]. Specific channels in this portion of T-Band spectrum are not contiguous and vary by metropolitan area and TV channels within that area. While a licensing freeze was not required by the law, the FCC placed a freeze on all new and expanded T-Band operations for public safety and industrial and business licensees. Immediately following the law's enactment, public safety communications experts concluded that solutions to challenges of spectrum relocation remain complex and costly for affected local and State public safety entities.

THE REPORT

In March 2013, NPSTC convened a T-Band working group to study the giveback and its implications for public safety communications, including the potential cost of relocation efforts (Figure 1)[4]. The full report is available on the NPSTC website, and cites costs, spectrum alternatives, and limited spectrum gains as potential limitations:

Figure 1. Breakdown of the $5.9 Billion in Costs



- **Cost:** Despite being a requirement of the Act, auction revenues may not cover costs related to spectrum relocation, which is estimated to exceed $5.9 billion (estimate from 2013). Additionally, auction proceeds do not consider private sector relocation costs, which may decrease the percentage of auction funding used specifically for public safety spectrum reallocation.
- **Spectrum Alternatives:** The law requires licensees to migrate from the T-Band to other, unspecified spectrum; however, insufficient alternatives leave few options for identifying replacement spectrum. The very high frequency (VHF), UHF, and 700/800 MHz bands have few available channels. Also, the Nationwide Public Safety Broadband Network (NPSBN) is not yet available to support existing mission critical voice operations displaced by T-Band relocation.
- **Gaining Public Broadband Spectrum:** Despite its initial intentions for repurposing, the relocation of public safety operations from the T-Band is unlikely to produce significant additional broadband spectrum for public use.

FCC ACTIONS

In response to Public Law 112-96, the FCC issued rules and guidance related to the required T-Band transition. On October 17, 2014, the FCC released the narrowband reserve channels (twenty four 12.5 kHz channels) to General Use under the administration of the Regional Planning Committees (RPC) for the benefit of state and local public safety users. On January 9, 2015, the FCC issued a Public Notice, announcing the following:

[1] See Public Law 112-96 enacted on February 22, 2012: http://www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf

[2] Electromagnetic spectrum, commonly referred to as spectrum, is the range of all possible frequencies of electromagnetic radiation. Radio spectrum or wireless spectrum refers to the part of the electromagnetic spectrum corresponding to radio frequencies in the range from 3 kHz to 300 GHz that may be may be used for wireless communication.

[3] The 11 affected T-Band markets include Boston, Chicago, Dallas, Houston, Los Angeles, Miami, New York, Philadelphia, Pittsburgh, San Francisco, and Washington, D.C.

[4] See the NPSTC T-Band Report: http://www.npstc.org/download.jsp?tableId=37&column=217&id=2678&file=T_Band_Report_20130315.pdf

- A five-year priority access window for T-Band incumbents to license the former reserve spectrum (from January 9, 2015, to January 9, 2020);
- The date for filing RPC Plan Amendments to incorporate the former reserve spectrum (June 2, 2015 [subsequently extended to October 30, 2015]); and
- The date by which certain licensees must reprogram their deployable trunked systems to operate on the former reserve channels (see FCC Public Notice DA 15-34 for specific dates)

The FCC required that T-Band incumbents seeking reserve channels (1) commit to returning to the Commission an equal amount of T-Band spectrum and (2) obtain RPC concurrence.5

FIRST RESPONDERS CONTINUE TO RELY ON LAND MOBILE RADIO

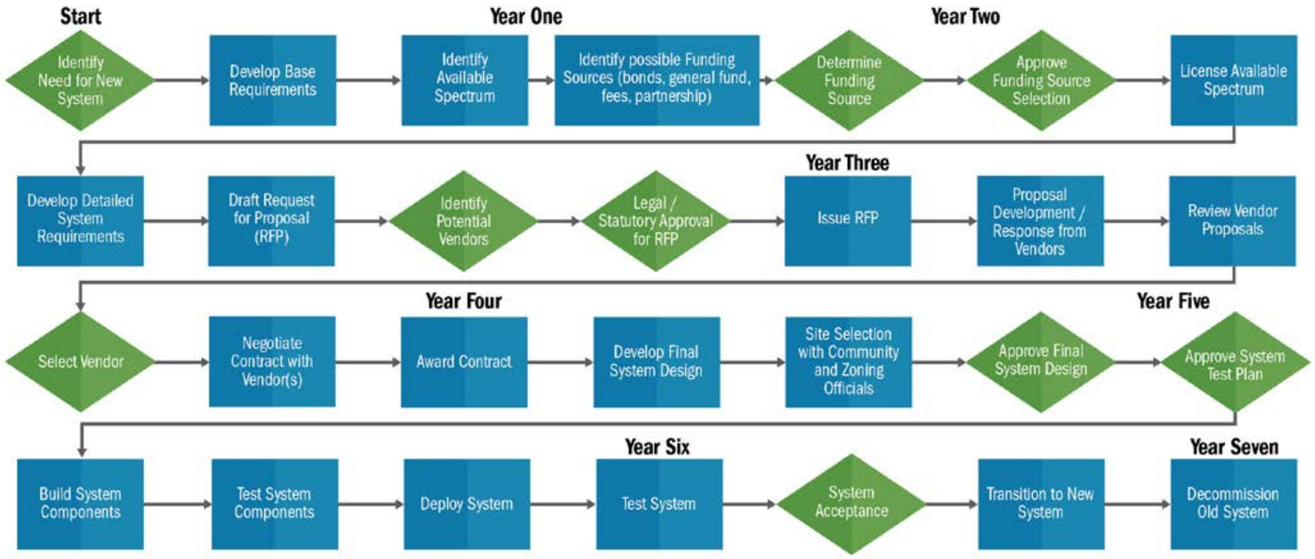
Although voice-over long-term evolution (VoLTE)[6] is successfully deployed by several major cellular networks, it is still unclear whether the 700 MHz NPSBN will be able to accommodate mission-critical voice for public safety users currently using the T-Band spectrum or have the capacity to concurrently support their voice and data communications requirements. Currently, wireless broadband technology does not support a mission critical voice capability (e.g., talk around/simplex/direct mode)[7] and is not a substitute for land mobile radio (LMR) mission critical voice. Therefore, first responders will continue to rely on LMR channels, such as those on the T-Band, as crucial components of their communications systems. The public safety community must work together to establish and test quality access, service, capacity, and a full set of public safety standards before achieving full convergence of LMR mission critical voice with broadband. Furthermore, the broadband network must be built out to provide coverage equivalent to that of today's LMR systems. Until then, LMR systems should be maintained and expanded in order to support first responders appropriately.

GRANT GUIDANCE

OEC has encouraged States to update Statewide Communications Interoperability Plans (SCIP) to address FCC directives affecting current or planned public safety communications systems, including T-Band migration, and has advised grantees to consult the FCC, their Statewide Interoperability Coordinator (SWIC), and their frequency coordinator during project planning, to ensure projects or upgrades planned for systems operating in the T-Band are coordinated and align with the State's migration plans.[8]

SAMPLE T-BAND GIVEBACK TRANSITION TIMELINE

The following is an example timeline providing proposed steps for transitioning to a new system.


Start
Year One
Year Two
Identify Need for New System
Develop Base Requirements
Identify Available Spectrum
Identify possible Funding Sources (bonds, general fund, fees, partnership)
Determine Funding Source
Approve Funding Source Selection
License Available Spectrum
Year Three
Develop Detailed System Requirements
Draft Request for Proposal (RFP)
Identify Potential Vendors
Legal / Statutory Approval for RFP
Issue RFP
Proposal Development / Response from Vendors
Review Vendor Proposals
Year Four
Year Five
Select Vendor
Negotiate Contract with Vendor(s)
Award Contract
Develop Final System Design
Site Selection with Community and Zoning Officials
Approve Final System Design
Approve System Test Plan
Year Six
Year Seven
Build System Components
Test System Components
Deploy System
Test System
System Acceptance
Transition to New System
Decommission Old System

[5] See FCC DA 15-34 published on January 9, 2015, at: http://www.fcc.gov/document/pshsb-provides-guidance-licensing-700-mhz-reserve-channels
[6] LTE is a 4G commercial cellular technology currently being deployed globally. LTE has been identified by the First Responder Network Authority as the "technology of choice" for the future NPSBN.
[7] U.S. Department of Homeland Security, Office of Emergency Communications, *Public Safety Communications Evolution Brochure*, 2014.
[8] FY 2014 SAFECOM Guidance at: www.safecomprogram.gov/ecg/2014_safecom_guidance_final.pdf