Encryption Considerations for Agencies using AWIN

This document was developed at the request of the public safety community by the Arkansas Interoperable Communications Executive Committee (AICEC) to provide supporting information for consideration and decisions at all levels of Arkansas 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 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.

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. 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, decisionmakers, 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 Arkansas Wireless Information Network (AWIN) is the statewide public safety radio system in Arkansas. Participation on AWIN is open to public safety agencies at both the state and local level. Many of these agencies combine local, regional, or statewide communications needs. Functions, such as public safety, public service, maintenance, and administration are often addressed in a jurisdictions talkgroup plan. 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," 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 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.

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 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. AWIN is digital and designed in compliance with applicable industry standards such as Project 25 or P25, which improves interoperability between radio systems. The P25 standard includes a strong encryption method known as the Advanced Encryption Standard, or AES. 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.

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 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. 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. Specifically, agencies must consider other agencies that have existing talkgroup permissions. Agencies should also consider encrypting only the transmit side of the conversation, so that an unencrypted subscriber could still be heard.

• **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. At least one Arkansas agency, in response to a lawsuit, makes clear audio available on a website after a specified period of time with an expiration that is specified.

• **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.

Putting Encryption in Practice

Pro Tip: Agencies using AWIN that make the decision to encrypt are not required to apply to AWIN for permission to encrypt.

Pro Tip: Agencies are encouraged to notify AWIN when they encrypt radios. This information will be used in two ways: AWIN System Technicians will use it when assisting users with radio issues, and communications technicians responding to disasters at the request of ESF#2 will use the information to establish communications plans.

Pro Tip: Agencies are not required to provide the tone and encryption keys to AWIN.

Pro Tip: Consider adding encryption features when new radios are purchased. AWIN users need to ensure that encryption codes (AES, ADP, and multikey) are purchased. These encryption codes can be added after purchase, however it is more costly to do so.

Pro Tip: Encryption resides in the radio; it does not reside on the talkgroup. When planning for encryption AWIN users should consider whether or not they have shared their talkgroups with other agencies. Encrypting these shared talk groups could result in the other agency missing critical communications.

Pro Tip: For best results and ease of operation, encryption should be pinned to the talk, not selectable by the user.

Pro Tip: Radios should be locked so that the programming cannot be read by anyone except a certified programmer with a passcode.

Summary

AWIN users 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?