Public Safety Land Mobile Radio Communications Security

Publication: January 2022
Cybersecurity and Infrastructure Security Agency

Table of Contents

WHY LAND MOBILE RADIO COMMUNICATIONS SECURITY

Reliable land mobile radio (LMR) communications are the backbone of public safety operations and key to mission success. The ability of responders to communicate and coordinate efforts during routine and emergency operations is the dominant factor in saving lives and protecting property. In recent years, *Communications Security*—COMSEC—has become an important element in the public safety environment. COMSEC focuses on the security of all elements of public safety communications, from the infrastructure of voice and data systems to communications facilities, radios, smartphones, tablets, and computers, as well as policies and procedures governing radio traffic.

This document focuses on the security of LMR systems, assets, and communications, with an emphasis on securing radio traffic with encryption.

> COMSEC is a component of Information Assurance that deals with measures and controls to deny unauthorized persons information from telecommunications and ensure the authenticity of such telecommunications.
>
> Computer Security Resource Center
> National Institute of Standards and Technology (NIST)

ELEMENTS OF LMR SYSTEM SECURITY

LMR system security relies on the same elements common to security of all communications systems, among them:

- physical security of infrastructure and assets
- physical security of communications facilities and personnel
- precautions against damage and operational impacts from natural disasters and intentional destruction
- security of sensitive voice and data traffic
- continual monitoring of system conditions
- regular comprehensive testing and assessment of system operability.

Included here are the careful selection of sites for towers and ancillary equipment; installation of adequate barriers (fencing, walls), signage, and surveillance devices to monitor sites; physically controlling access to public safety facilities housing communications personnel and equipment; implementing encryption to protect sensitive mission-critical voice and data communications; and establishing policies and procedures to ensure everyone responsible for and involved in communications is functioning in a manner that reinforces system security. A discussion of all these elements is beyond the scope of this document. Nonetheless, system designers and administrators need a solid grounding in the principles of system security and are referred to the Cybersecurity and Infrastructure Security Agency document "Cybersecurity and Physical Security Convergence" for detailed information.

SECURING LMR COMMUNICATIONS

Much emphasis on COMSEC arises from public concern over privacy. The requirement to safeguard protected health information (PHI) and personally identifiable information (PII) broadcast during a public safety incident is important. Public safety officials have their own security concerns. The proliferation and availability of web-based apps, frequency jammers, radio cloning devices, and encryption-breaking software—and even more powerful technologies on the horizon—challenge public safety's efforts to protect sensitive transmitted information. In the aftermath of a crime, how can law enforcement officials protect details regarding a search area? During a disaster, how do rescue teams share critical information free from eavesdropping by media or private citizens, which could lead to news coverage or crowds that disrupt life-saving operations?

COMSEC recognizes that sensitive information needs as much protection as public safety personnel and assets. While agencies have long implemented policies and procedures for general operational security, their focus now

includes protecting sensitive information and the wired and wireless mediums used to transmit, receive, and share such information. The objectives are:

- secure citizen PHI and PII
- protect law enforcement information regarding sensitive operations and investigations
- secure critical operational information during routine and emergency response to incidents, special events, and disasters
- protect information that could be used to threaten, injure, or kill public safety personnel
- anticipate technologies that could compromise the privacy, confidentiality, and authenticity of information resources.

An essential security technology that meets all these objectives is *encryption*.

THE NEED FOR ENCRYPTION

Encryption is a technology that scrambles transmissions in a way that only authorized personnel can receive them in an intelligible form. Unauthorized persons who intercept the transmissions hear only noise or nothing at all. What is the value of protecting transmissions with encryption? Consider some real-life examples:

- During a recent protest, law enforcement personnel were called to control violence in a downtown section of a major city. Illicit actors using web-based applications listened to law enforcement channels and distributed information to the crowds, facilitating looting, arson, and assaults on law enforcement personnel. This breach of communications security compromised citizen and officer safety and disrupted law enforcement planning and execution of an appropriate response to the civil unrest.
- Criminals monitoring unencrypted radio traffic challenge officer and citizen safety. Along the Southwest border and in other jurisdictions around the country, technologically sophisticated criminals routinely sift through law enforcement transmissions to gather information on tactical operations, locations of law enforcement units, and citizen PII—driver license numbers, birth dates, etc.— putting citizens at risk of identity theft and jeopardizing officer safety and operations.
- During a Super Bowl, a copy of the security agencies' communications plans somehow leaked into the public domain. A local hacker created a web-based listing of all the channels and the intended channel usage, including assigned users. There were also links to online stores that could provide scanner apps that would permit anyone with a smartphone, laptop, or tablet to listen to any of the unencrypted talkgroups/channels.
- In a Southwestern state, law enforcement officers responding to an active shooter incident across several locations quickly developed information about the suspects, their probable location, and potential new targets. When investigators confirmed the suspects' location, they broadcasted the information over an unencrypted dispatch channel to patrol officers and tactical teams. Media outlets were listening to the dispatch channel and set up for a live broadcast at the suspects' location before law enforcement teams arrived. The situation posed a significant safety issue for the media crews and, by eliminating the element of surprise, put the officers at risk and compromised the tactical plan initiated to take the suspects into custody.

MODERN ENCRYPTION

More than two thousand years ago, Julius Caesar developed a substitution cipher (substitute *r* for *g, t* for *o*, *c* for *a*, etc.) to encode written orders sent to his field commanders. Only commanders who had Caesar's encryption key (list of substitutions) could decipher the messages. Today, encryption of digital communications works in a

similar way, except complex algorithms (computer instructions) automatically perform the encrypting for the sender and decrypting for authorized recipients. If a high-quality algorithm is used (see The Encryption Standard below), the resulting encryption is infinitely more complex and secure than Caesar's simple substitution scheme and essentially unbreakable even by today's most sophisticated computers. Yet the process is transparent to LMR users in the field. It is a complex technology that requires thorough understanding, methodical implementation, and careful, persistent management. Properly implemented, however, encryption offers agency officials and frontline responders both the protection of and confidence in the security of sensitive transmissions.

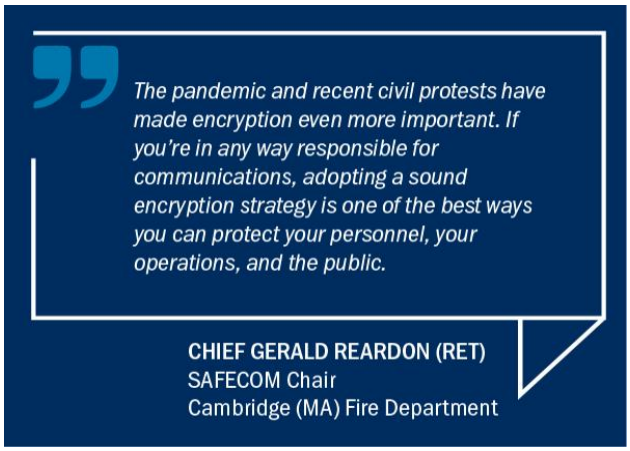
BALANCING THE USE OF ENCRYPTION

Decision-makers should understand that many public safety channels and talkgroups may not require encryption. By determining in the planning stages which talkgroups, radio channels, and types of information should be encrypted, agency and jurisdictional leaders can implement an effective encryption strategy.

Public safety agencies and government leaders must make informed choices to protect critical and sensitive information from unauthorized reception while comprehensively protecting public safety operations. Equally important are alternatives that will permit sufficient transparency to still allow some types of reception for a "citizen's right to know."

BLENDING ENCRYPTION AND INTEROPERABILITY

Over the past two decades, agencies nationwide have worked hard to achieve interoperability in-house and among mutual aid partners. They have developed shared systems and networks, policies, and procedures to ensure that when they must work together, they can communicate with each other. These same agencies now realize they need to protect sensitive information they share during multi-jurisdictional incidents and mutual aid operations. Yet many remain concerned that encryption and other security measures could disrupt interoperability and increase costs. This can, in fact, happen if these measures are poorly implemented or managed; however, if all stakeholders approach security and encryption in the same manner they approach interoperability, the results can be equally successful.



The solution lies in agencies working with both their components and mutual aid partners to develop shared encryption policies and procedures and to establish mutual network security and encryption management practices. For example, agencies can share encryption keys to ensure seamless interagency communication on predetermined encrypted channels or talkgroups. Arrangements like this require agency leaders to cooperatively decide on the selection, implementation, management, and governance of a uniform encryption strategy and the infrastructure to share information securely. Policies must ensure that the personnel responsible for deploying and managing the strategy are fully qualified with the technical knowledge and skills required. These subject matter experts should be involved in addressing critical decisions, so agency leaders understand the value, risks, costs, and operational impacts of encryption and are able to effectively explain them to elected officials.

THE ENCRYPTION STANDARD

Project 25 (P25) Accredited Technical Standards[1] make reliable interoperability possible, and P25 specifies the Advanced Encryption Standard (AES) as the only truly secure encryption algorithm for LMR systems. AES is recognized worldwide as the premier encryption algorithm for wired and wireless voice and data communications.

Like other technologies, digital encryption has evolved. In the early 1970s, IBM developed the Data Encryption Standard (DES), and in 1977, NIST (then the National Bureau of Standards) adopted and published DES as an official Federal Information Processing Standard (FIPS). In the late 1990s, DES had been "broken" by increasingly advanced computers and was no longer reliable. In 2001, NIST adopted and published AES as a more secure algorithm (FIPS 197). Today most federal agencies that encrypt information use AES-256, and the P25 standards recognize only AES as a reliable encryption algorithm.

Some manufacturers still offer DES, as well as alternate non-standardized and proprietary "privacy" features, in their LMR equipment, often at no cost. These alternatives can be easily compromised in minutes using consumer-grade computers. At the same time, because it is a federally provided encryption algorithm, AES is provided to manufacturers at no cost, except the cost for certification testing. As a result, many manufacturers offer AES at reasonable cost to their customers. Procurement officials should check with vendors to determine if AES is available and at what cost. Note, however, that while the cost for AES itself can be minimal, implementing it requires additional investments in encryption services and encryption-capable equipment.

SUMMARY

A comprehensive, effectively managed LMR COMSEC posture ensures the security of infrastructure, facilities, assets, and personnel, as well as the confidentiality and integrity of sensitive wired and wireless public safety communications. Together, physical security, cybersecurity, and strong encryption coupled with stringent policies, methods, and procedures can provide adequate protection for LMR systems and the public.

Encryption is among COMSEC's strongest tools, and encryption using the AES algorithm is the only reliable method available to secure public safety wired and wireless communications. To successfully implement and manage an encryption strategy, agency leaders must understand the value, risks, costs, and operational impacts of encryption and ensure that personnel responsible for day-to-day encryption operations have the technical knowledge and skills, resources, and policies and procedures they need. Additional information is available at cisa.gov/publication/encryption.

For more information or to seek additional help, contact the Federal Partnership for Interoperable Communications at FPIC@cisa.dhs.gov.

[1] P25 is a suite of standards for interoperable two-way digital LMR services for public safety. The P25 Technology Interest Group website provides information on all topics concerning the P25 Suite of Standards at: project25.org.