Considerations for Encryption in Public Safety Radio Systems

Sept 2016

SAFECOM

Federal Partnership for FPIC Interoperable Communications

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