PUBLIC SAFETY
PSWN PROGRAM
WIRELESS NETWORK

Saving Lives and Property Through Improved Interoperability

Security Issues Report—Impediments and Issues on Using Encryption on Public Safety Radio Systems

FINAL

March 2002

Table of Contents

EXECUTIVE SUMMARY ES-1
1. INTRODUCTION 1
2. LEGAL, REGULATORY, AND POLITICAL ISSUES 3
2.1 The Need for Encryption 3
2.2 Encryption and Interoperability 4
2.3 The Freedom of Information Act 4
2.4 The Privacy Act 4
2.5 Presidential Decision Directives and Authorities 5
2.6 The Politics of Encryption 6
2.7 Conclusions 6
3. PUBLIC SAFETY OPERATIONAL ISSUES 7
3.1 Perceptions About Encryption in the Public Safety Community 7
3.2 Perceptions About Encryption in the Public Arena 8
3.3 Separating Fact From Fiction About Encryption 9
3.3.1 Experiences in Switching from Analog to Digital Communications 9
3.3.2 Security, Making the Digital Switch, and Other Thoughts on Encryption 11
3.4 Conclusions 16
4. FISCAL CONSIDERATIONS 18
4.1 Fiscal Issues 18
4.2 Technological Advances 18
4.3 Cost to Implement 19
4.3.1 New System Development Cost 19
4.3.2 Aftermarket Implementation 20
Estimated Cost 21
5. SUMMARY 23
6. ADDENDUM 26
6.1 Impact of the Terrorist Attacks on Opinions Regarding Communications Security and Encryption 26
6.2 Encryption and Security 26
6.3 Conclusion 28

EXECUTIVE SUMMARY

The intent of this report is to further identify and qualify issues and challenges associated with the development, deployment, and decisions regarding the use of encryption technologies within the state and local public safety community.

This examination presents factual information and dispels common mis-information about the use of encryption technologies, potential legal ramifications, and operational considerations. The report strives to provide additional insight regarding public safety agency's views and decision factors regarding the procurement and deployment of encryption technologies in land mobile voice radio systems.

Hopefully, this report provides beneficial information that may lead state and local agency administrators to further consider the inclusion of encryption technologies within existing or new communications system projects. Also, the presentation of cost information may assist agencies and their governing bodies to fully appreciate the costs, both human and equipment, required to facilitate the deployment of encryption.

The report also considers the uncertain legal landscape and operational difficulties associated with using encryption on a public safety communications system. These issues may require further analysis, policy and procedure development, community and agency collective actions, and potentially legislative actions to provide an acceptable balance of public safety communications protection and the publics "right to know."

The fundamental issue explored in the report is the disparity in the use of encryption by federal agencies and by state and local agencies. State and local agencies continually indicate a desire to implement encryption technologies to enhance communications capabilities but most ultimately do not.

Existing and pending encryption technology developments are discussed and the existing land mobile radio (LMR) standards are defined. Current legal, regulatory, and political issues surrounding the use of encryption are reviewed and discussed. Specific operational references, viewpoints, and antidotal information obtained from state and local public safety agencies are presented.

This report presents cost information obtained through contacts with state and local agencies, primary manufacturers, and after-market vendors. This information is intended to provide a benchmark of potential equipment and support cost that may be realized when procuring and maintaining encrypted systems.

The analysis confirmed much of what had been previously suspected regarding the impediments of the deployment and use of encryption in state and local systems. Specifically, the information indicates—

- The cost of procuring, deploying, and managing encrypted systems is the overwhelming reason for not embracing encryption.

- State and local agencies indicate that the return on investment (ROI) is negligible, making it very difficult to acquire funding.

- State and local agency communications operational and capital budgets are severely limited, and agencies usually view encryption as a "luxury" item that they decline in lieu of more infrastructure or subscriber units.

- Many state and local agencies consider interoperability communications very important and perceive the use of encryption as limiting or excluding these communications.

- Public law, policy, and public perception of state and local government use of encryption remains ambiguous and uncertain.

- State and local public safety agencies are desirous of definitive judicial and/or legislative findings or actions regarding the authorized uses of encryption.

- The terrorist attacks of September 11, 2001, have not substantially influenced the public safety community viewpoint on the use of encryption.

State and local agencies must continue to pursue additional funding opportunities to support the inclusion of encryption technologies on existing and new communications systems. Government at all levels should be compelled to establish funding programs to acquire encryption technologies for new system projects and to find reasonable opportunities for legacy environments.

All public safety agencies must remain vigilant and participatory with regard to the legal issues surrounding the use of encryption. The existing statutes are ambiguous at best and are open to a variety of interpretations. This undefined legal position contributes to agency uncertainty when considering the procurement of encryption. Therefore, governments at all levels should consider proactive statutes that strike a proper balance between protecting critical public safety communications and preserving civil liberties.

The technologies of encryption continue to evolve and advance, and the National Institute of Science and Technology (NIST) has accepted a new, more robust standard. The new standard will require acceptance and incorporation by the various LMR standards development organizations (SDO) as well as the vender community. LMR vendors and manufacturers should be compelled to quickly adopt the new, more rigorous standards with sensible and affordable migration strategies. The adoption of the Federal Information Processing Standards (FIPS) 197 for the Advanced Encryption Standard will eventually replace the use of the current Data Encryption Standard in the LMR environment.

The advent of new standards will continue to complicate the ability of agencies to interoperate both in clear mode and in encrypted modes. The SDOs, public safety, and vendors must work diligently to employ standards that provide the highest levels of encryption capability while ensuring adequate interoperability. The Project 25 User Needs Subcommittee and the Telecommunications Industry Association (TIA) has identified the need for the more robust encryption algorithm and have taken steps to ensure a timely and graceful migration while continuing to provide a capability for interoperability with existing systems.

The Users Needs Subcommittee revised the published Project 25 Statement of Requirements to state “For interoperability purposes, all Project 25 equipment using Type 3 encryption shall be capable of operation using the DES algorithm, or an encryption algorithm compatible with the DES. An example of an algorithm compatible with DES is the Triple Data Encryption Algorithm (TDEA) using Keying Option 3 (a keying bundle wherein all keys are identical).

The SOR further states "The TDEA shall be implemented to allow a graceful, cost-effective transition to the Advanced Encryption Standard (AES) algorithm under development by the National Institute for Standards and Technology (NIST)."

Further information and education should be provided to the public and media in order to gain support for necessary encryption of communications in these uncertain times.

1. INTRODUCTION

Public safety voice radio communications may routinely contain sensitive and vital information. Often, preserving the private nature of this information is essential to the protection of life and property. Disclosure, modification, or interception of this information could severely impact public safety operations and potentially endanger both public safety personnel and citizens. Because of these potentially serious implications, the public safety community has recognized that often these communications require protection. As technologies in land mobile radio (LMR) have developed, so have the opportunities and challenges to safeguard voice radio communications.

One means of improving security is by adopting system-level technology that is more private by its very nature. Examples of this technology have included trunked radio systems and digital radio systems. Originally, trunking offered a perceived level of privacy because it randomly moved the radio message from channel to channel. Digital radio technology offered a level of privacy because scanners and receivers commonly available to the public operated only in analog mode and were unable to translate any digital transmissions into intelligible messages. However, scanners capable of tracking messages on trunking systems have been available for several years now, and at least one manufacturer is developing scanning equipment capable of receiving and unscrambling a digital voice message. The advent of this new scanning technology will eliminate the perceived level of privacy that digital trunking system users have enjoyed for the past several years. The only technology that will provide reliable, secure communications is encryption.

Encryption, which is the process of transforming a plain message into unintelligible code, has been used in radio messaging since before World War I. The German military used cryptography to encode its messages. Of course, with survival at stake, the allied forces developed the knowledge needed to break the German code. The French began recording detail about German radio traffic early in the war, including information such as signal strength, length of messages, and characteristics of content. The French were unable to decode the messages at the time; however, within a few years, they began to successfully decipher the previously recorded German messages. This success was invaluable to the French in assessing the thoughts, the troop strength, and the patterns of movement their enemy had adopted. These efforts contributed significantly to the allied victory.

However, many agencies in the public safety community in the United States have been reluctant to employ encryption within voice communications systems. The development of the Data Encryption Standard (DES) in 1977 provided an opportunity for this technology to be considered for public safety applications. Currently, DES is the accepted standard for public safety encryption under the Telecommunication Industry Association/ Electronic Industry Alliance Standard 102 (TIA/EIA 102).

The new Advance Encryption Standard (AES) promises more robust encryption algorithms superceding those of the DES and Triple DES that has become the standard in the information technology (IT) community. With its acceptance and authorization by NIST on

November 26, 2001, AES has been accepted as the new encryption standard by TIA/EIA for incorporation into LMR communications systems. This new standard allows for a migration path from DES to AES and requires new equipment to be backward compatible to existing equipment. Despite the decision that all federal law enforcement agencies would incorporate encryption in their communications systems, the public safety community at the state and local level has been less likely to do so.

The PSWN Program has determined that examining the attitudes and policies of state and local public safety agencies as they pertain to encryption may provide some insight into the reluctance and perhaps raise awareness about employing encryption technologies in their future communications systems. This examination, titled *Security Issues Report—Impediments and Issues on Using Encryption on Public Safety Radio Systems*, is a security issues report that takes a high-level look at the issues that state and local officials face regarding the use of encryption in public safety communications systems. This report will focus on—

- Legal and regulatory issues pertaining to encryption
- Public safety operational issues
- Fiscal issues regarding the deployment of encryption technologies.

By examining these issues—some real, some perceived—the Public Safety Wireless Network (PSWN) Program hopes to provide government leaders with the information they need to make sound decisions in this critical area.

2. LEGAL, REGULATORY, AND POLITICAL ISSUES

Currently, most state and local public safety agencies broadcast their day-to-day and critical radio communications in clear voice mode, which enables individuals who own radio scanner receivers to monitor their messages. Because these communications are in clear voice mode, there is no expectation of privacy for the conversations that occur. As public safety agencies move to protect these communications, the question arises whether the public has a legal right to monitor these transmissions.

Local, state, and federal laws and regulations give public safety agencies a great deal of latitude in the manner in which they can conduct their wireless communications. No local, state, or federal laws specifically prohibit or require the use of encryption by public safety agencies. In recent years, several states, most notably Michigan and Florida, have attempted to enact state laws restricting the ability of the press and citizens to monitor public safety radio transmissions in order to enhance safety of public safety personnel. None of these efforts has been successful. However, existing statutes do deal with related issues, such as the need for encryption, interoperability, and public access to records of encrypted communications. The purpose of this section is to provide an overview of those issues and the political implications of encryption.

2.1 The Need for Encryption

According to the United States Code,[1] it is legal for any person to intercept public safety communications that are "readily accessible to the general public." Therefore, public safety communications are not protected from interception either technically or legally unless steps are taken to protect the communications and make them not "readily accessible." In effect, the message lawmakers are sending to public safety officials is if they want to conduct communications that require privacy, they must take affirmative steps to make it private. Interception of encrypted public safety communications may be illegal under the United States Code; however, it should be noted that there has never been a judicial ruling on this issue by any Federal Court. There have also been many documented cases of the criminal element intercepting public safety communications in order to escape detection and arrest for illegal activities.

In 1999, the PSWN Program recognized that the security risks that faced public safety LMR systems were increasing. In response, the PSWN Program published a document titled *Land Mobile Radio System Recommended Security Policy*. The document outlines a recommended security policy to be used by local, state, and federal public safety agencies to mitigate these risks. The Security Policy recommends that encryption be used on all public safety LMR systems to ensure the protection of the information they carry.

[1] 18 U.S.C. 2511. *Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited.* Specifically, "(2)(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—(ii) to intercept any radio communication which is transmitted—(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public.

2.2 Encryption and Interoperability

Although encryption may be needed for secure communications, it can be a hindrance to interoperability. The Federal Communications Commission (FCC) has recognized this problem and has limited the use of encryption on the 700 megahertz (MHz) public safety Interoperability channels.[2] Specifically, the FCC will only allow the TIA/EIA 102 Project 25 Phase I DES encryption protocol on interoperability spectrum. In addition, the FCC has prohibited the use of encryption on the two 700 MHz public safety Interoperability calling channels. Additionally, no other FCC-mandated regulations on any other public safety spectrum either require or prohibit the use of encryption.

2.3 The Freedom of Information Act

The Freedom of Information Act (FOIA) requires that recorded communications, like all other government records and documents, be available to the public upon request.[3] Additionally, states and localities may have their own laws and ordinances that require even greater openness to the public. The provisions of the FOIA represent the minimum amount of public access that state and local public safety agencies must provide. Therefore, although encryption will ensure the security of the information when it is passed on the network, the agency may be required to disclose any records of the information at a later date pursuant to the FOIA.

Public safety agencies should have a process in place by which they regularly review their records to determine which documents they will make available to the public. If a public safety agency makes a record of communications that are encrypted, that record, like all other documents, may be subject to FOIA requests by the public and should be reviewed. There are exceptions to the FOIA. The exceptions that may apply to public safety communications are those that refer to personal and medical information, and certain law enforcement related information. The agency whose records are being requested bears the burden of proving that any records are exempt from disclosure. Information that may be withheld under the FOIA may be disclosed by an agency as a matter of administrative discretion—if not explicitly prohibited by law, and if the agency determines such disclosure would not cause foreseeable harm.

2.4 The Privacy Act

The Privacy Act prohibits a governmental agency from disclosing "any record regarding an individual to any person or another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the records pertain."[4] An agency must allow individuals the right to review records that pertain to them.[5] In addition, an agency is required to

[2] Forth R&O, *In the Matter of the Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010,* WT Docket 96-86, rel. January 17, 2001.

[3] 5 U.S.C. § 552.

[4] 5 U.S.C. §552a(b)

[5] 5 U.S.C. § 552a(d)(1).

maintain only records of individuals that are essential to the functioning of the agency.[6] An agency shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."[7]

If public safety radio communications were encrypted and the transmissions ceased to be open, possible violation the Privacy Act might arise. A balancing test, likely devised by the legislature and affirmed by judiciary would need to be applied between the public's right to know and the individual's right to privacy. Given the wealth of personal information included in public safety radio communications and 911 calls, a person mentioned in a communication not accessible by scanner could assert a strong privacy right regarding the communication.[8] There is also the question regarding the expectation of privacy of the public safety personnel who are making the voice communications. If public safety radio transmissions were encrypted and unavailable to the general public or news media, it is quite conceivable that the transmissions would fall under FOIA and/or the Privacy Act. Whether or not the transmissions or transcripts would be released would have to be balanced against the public's right to know and the privacy interests of the individuals involved.

2.5 Presidential Decision Directives and Authorities

A number of Presidential Decision Directives (PDD) have been promulgated to promote further cooperation within the intelligence community and with law enforcement authorities.

PDD-63 calls for a coordinated public and private national effort to develop a security framework to protect the critical infrastructure,[9] including the telecommunications, banking and finance, energy, transportation, and essential government services sectors. Although PDD-63 does not specifically call for the encryption of radio communications, the requirement to protect critical infrastructures seems to imply that very idea. The success of PDD 63 depends on the creation of a strong partnership among the Federal Government, the business community, and state and local governments. The combined effort requires public agencies and their private sector counterparts to coordinate and assist one another with the protection of critical assets. In light of the bombings of the World Trade Center in 1993 and Oklahoma City Federal Building in 1995, and the terrorist attack against the Pentagon and the World Trade Center in 2001, the threat is indeed real.

As the likelihood of terrorist activities increases, it will be incumbent upon government to further protect its citizens. A significant threat to security and public safety operations is possible through the exploitation of the country's public safety communications systems whether

[6] 5 U.S.C. § 552a(e)(1).

[7] 5 U.S.C. § 552a(e)(7).

[8] *See* Jamison Prime at 362 (providing and elaborating on the pursuing argument).

[9] A White House white paper defines critical infrastructure as "those physical and cyber-based systems essential to the minimum operations of the economy and government." White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (May 22, 1998).

they are LMR or computer information systems. Thus, the precautions that the public safety community takes to secure its communications systems may indeed pay dividends in the future.

2.6 The Politics of Encryption

Although most laws and regulations support the right of public safety agencies to encrypt their communications, several constituencies have a vested interest in preventing the encryption of communications that are currently open to the public. These groups have the potential to influence the political environment in a way that could ultimately restrict the encryption of public safety communications.

The group most associated with monitoring voice communications made by public safety organizations is the news media. The news media rely on scanners to determine whether an event may be newsworthy or whether a public safety incident is occurring. The general public also monitors public safety communications on a regular basis. This latter group is mainly "scanner enthusiasts" who maintain that they listen to public safety communications to keep abreast of developments in their communities and to be a watchdog for potential misconduct. As taxpayers and public interest advocates, these groups believe they have a right and a genuine need for access to public safety communications. It is possible that these groups and individuals could mobilize political resistance to the deployment of encryption that results in restrictive laws in a particular state or locality. Section 3 of this report discusses this issue in greater detail as it relates to operational issues.

2.7 Conclusions

If a public safety radio message is transmitted in clear voice mode, it is presently considered public information. Therefore, if there is a desire or need to safeguard these transmissions, encryption of the information is the only option. Presently, no local, state, or federal laws prohibit the use of encryption technology. Encryption technologies deployed on LMR systems only protect the information at the time of the communications. Any record of the encrypted communications, like all government documents, is subject to discovery through the FOIA. Finally, although federal law is consistent throughout the Nation, system planners should evaluate the political and legal environment of their state or locality. Political pressure in some jurisdictions could result in enactment of laws and regulations that limit the use of encryption by public safety agencies.

Public safety agencies contemplating deployment of encryption components or services within new or existing radio systems should thoroughly investigate applicable local, state, and federal statutes, and any new decisions from the courts. In addition, appropriate discussions with agency legal representatives should occur to determine the associated risk in using encryption technologies.

3. PUBLIC SAFETY OPERATIONAL ISSUES

This section addresses the operational issues related to using encryption on public safety radio systems. First, many of preconceived ideas of the public safety community and the public at large regarding encryption are explored. The report then moves on to the results of interviews held with public safety radio system managers to gain their insights into the potential uses of encryption technologies.

3.1 Perceptions About Encryption in the Public Safety Community

There are many preconceived perceptions about using encryption in public safety communications. These perceptions can be grouped into two general categories of advantages and disadvantages.

Among the perceived advantages are the following—

- Encryption is regarded as a means of enhancing law enforcement officer safety. Encryption accomplishes this by allowing uniformed officers to move about on patrol or in response to calls without the public's knowledge of these activities. This prevents officers from being drawn into ambush situations.

- Encryption improves the security of covert or tactical operations. This view stems from experience in specialized enforcement activities, such as vice, narcotics, or arson investigations, warrant services, or high-risk criminal apprehension operations. Using encrypted communications allows investigators the freedom to discuss suspects, activities, locations, and arrest plans on the air without fear that this traffic will be intercepted by criminal elements directly or indirectly involved. It also may minimize the need for alternative communications devices. Undercover officers are protected from having their identities exposed.

- Encryption defeats criminal elements that would otherwise use radio receiver equipment to protect illegal enterprises or operations. Burglars, auto thieves, robbers, and others involved in committing crimes in fixed locations have been known to monitor scanners to track police movements nearby and to learn when their own activities have been detected in order to gain time for their escape. Presently, encryption prevents the use of scanners for this purpose.

Among the perceived disadvantages are the following—

- Encryption prevents the public from being informed about activities in their neighborhoods. Significant fires, natural disasters, fleeing criminals, and other emergencies or events may affect the safety of residents who may be either forced to evacuate on short notice, or to remain confined to their homes until the danger has passed. In the former scenario, informed residents are better prepared to leave and are less likely to resist the advice of emergency responders who tell them when it is time to leave. In the latter scenario, informed residents are less likely to step outdoors into peril from a desperate felon who may use an innocent person as a hostage to make an escape, or to be caught in the crossfire between law enforcement and wanted fugitives. In remote areas especially, scanners often provide the neighborhood news to residents.

- Encryption impedes volunteers—the largest segment of firefighters and emergency medical technicians in the United States—from monitoring and responding to emergency calls unless expensive radio equipment is available to them. In many communities across the country, radio paging supplements other notification methods, including scanners and "house sirens."[10] This is primarily because of the expense and accountability issues involved in issuing two-way radios to volunteer staffs. Many community-based public safety agencies, such as volunteer fire departments or rescue squads, lack the funding necessary to provide an adequate number of radios for official vehicles, much less for individual members. In small career departments, off-duty personnel are often subject to call-back in the event of significant incidents, and they too rely upon scanners or other inexpensive radio devices to receive these notifications.

3.2 Perceptions About Encryption in the Public Arena

Two other segments of society openly oppose encrypted public safety communications. They are the media and scanning enthusiasts. The media demand open and unlimited opportunities to scan public safety radio communications in order to learn about potential news stories. Scanning is considered a means of electronic newsgathering (ENG) in the industry. The media also generally assert that scanning preserves the public's "right to know." Scanning enthusiasts, by their very nature, are opposed to any system architecture or technological method that restricts reception of messages. Many scanning enthusiasts maintain that they have rights as taxpayers (who have paid for their public safety resources—including communications systems) to monitor public safety radio traffic. Some scanning organizations exist out of an interest to assure that government is operating in an above-board manner and in the best interests of the public they serve. These organizations commonly have members who scan, receive messages, transcribe traffic, and post segments on the World Wide Web (WWW) for all to see. They perceive their work as doing public good.

As strong as perceptions and opinions may be about public safety communications, some factual issues potentially impact the use of encryption in state and local public safety communications systems. These issues include—

- Legal challenges by media or scanning organizations

- Costs affecting acquisition and operation of encryption technologies

[10] An outdoor siren that is used to alert volunteer firefighters or emergency medical technicians to respond to their firehouse or rescue squad station for an emergency call.

- Impact on interoperability (different agencies using different encryption systems and keys)

- Benefits of public reception being adversely impacted.

The four primary benefits of public reception are—

- The media can immediately alert the public in areas impacted by significant events.

- Volunteers can readily receive notifications and updates about emergency calls.

- Citizens can monitor their public safety providers to assure that they are working for the public good.

- Citizens who monitor public safety communications may assist law enforcement agencies in the detection and apprehension of the criminal element.

3.3 Separating Fact From Fiction About Encryption

Based on these premises, the PSWN Program conducted research to either confirm or debunk all of the perceptions described above. Included in the research were interviews with radio system managers at the state and local levels to obtain information on their particular communications systems, and their personal viewpoints on encryption. These interviews were conducted based on prior experiences with agencies that were involved in planning encryption in the next generation of communications, or those that had encountered similar concerns when switching from analog to digital communications systems. In this latter circumstance, the radio system managers had, to some extent, already encountered these perception issues.

3.3.1 Experiences in Switching from Analog to Digital Communications

A large East Coast municipal agency began to prepare for the deployment of analog to digital communications system in the late 1990s. Internally, some high-ranking law enforcement officers were concerned about the loss of the ability to monitor radio traffic from scanners or other types of radio receivers. Their primary concerns were that citizens and other area law enforcement agencies should be able to monitor radio traffic to enhance personal and officer safety. The pending switch from a ultra high frequency (UHF) radio system to an 800 MHz radio system concerned them so much that they made a formal proposal to simulcast radio traffic on the new 800 MHz trunked system and on either another UHF conventional system or a very high frequency (VHF) conventional system. Senior agency officials tasked the communications administrator with responding to this proposal.

In the end, it was determined that there was no operational benefit to simulcasting. Adjacent law enforcement agencies would continue to receive official notifications of significant events for which their assistance was needed via direct communications between affected communications centers—as had always been the agency's official tactic. The costs and feasibility of a separate simulcast network were deemed too daunting. The estimated cost, in

1998, to build such a system was between $121,000 and $237,000, depending on whether any of the legacy system equipment and transmitter sites could support both the digital and analog systems. All of this assumed that the additional UHF or VHF channels could be obtained. This agency, based in a county close to a major metropolitan area that was also the base of operations for a number of state and federal law enforcement functions, had found that obtaining additional frequencies in these bands was not possible. This factor was the primary driving force in the agency's move to 800 MHz service. The only remaining issue to be addressed by the proposal was citizen and media access. This issue came to a head in the beginning of the 21st century, when members of the local broadcast media threatened a legal challenge unless some means of system access was made available. The solution proposed was to develop a Memorandum of Agreement between the agency and interested media outlets to allow them to purchase digital radio receivers licensed by the agency.

In 1996, a Midwestern locality also prepared to switch from analog to digital radio service. This city developed an 800 MHz Access Policy that identified the conditions under which parties not authorized to talk on their communications system could access their system to listen. The policy provided that authorized listeners would be granted access to monitor "routine" public safety talk groups, which were identified by the communication systems administrator. The system administrator was also given complete control over all equipment used by the authorized listeners. To gain access, potential listeners were required to apply for a permit. The permitting process provided that the city was not responsible for any costs or expenses related to listeners gaining access to the system. The city also retained the right to determine who could listen, based on whether the listener's access would benefit public interests. The city also retained the right to terminate any permit for breach of permit and the right to interrupt or terminate listener access. These caveats allowed the city to grant some access without losing control over system properties and features.

As early as 1994, a West Coast city recognized that switching from a conventional analog communications system to a trunked digital communications system would cause problems for members of the media. This city established a working group consisting of representatives of the public safety agencies participating in the new system, and representatives of the local print and broadcast news agencies, as well as local government leaders. This working group was tasked with developing an alternative means, in lieu of scanners, for the media to learn about significant events. There was some common ground that the various group members readily agreed upon. This included a decision regarding which talk groups could and could not be monitored by the media. Banned from monitoring was radio traffic on talk groups serving fire, arson, vice, and narcotics investigations, internal security elements, and tactical operations. Approved were talk groups used in support of routine firefighting and law enforcement operations and disaster response. In fact, it was this latter talk group that the group agreed should specifically be monitored by the media in order to quickly gain valuable information to use in informing the public of such situations as plane crashes and earthquakes. The access agreements eventually crafted by this working group were amended to include provisions for citizen access. This city clearly supported a balance between the public's right to know and public safety's need to protect its personnel and critical operations.

3.3.2 Security, Making the Digital Switch, and Other Thoughts on Encryption

The PSWN Program contacted two municipal radio system managers and two state radio system managers responsible for large multiple agency public safety communications to obtain their viewpoints on security and encryption. A profile was prepared of these systems, some of their communications security measures, and their interoperable communications capabilities and applications. Each manager received a listing of eight statements about encryption and was asked whether he or she agreed or disagreed with each. The radio manager was then asked to provide views that supported his/her positions on key encryption issues.

The first communications system serves more than 2,000 public safety users, including town, city, county, and regional police officers, sheriffs, and the largest fire and rescue organization in the state, located in a large Mid-Atlantic county. The system in place is a conventional analog communications system, transitioning into a new trunked digital communications system operating in the 800 MHz band. The new system meets the TIA/EIA-102 standard and is compliant with the Associated Public Safety Communications Officials (APCO) P25 system standards. The new system also incorporates cellular digital packet data (CDPD) technology for mobile data transmissions.

This new system uses several security measures including voice privacy, encryption, and a manufacturer's built-in multikey system. The new system is also capable of inhibiting lost or stolen radio equipment.

Interoperability is also a feature of this new system. There is a constant employment of interoperability for local agencies in this system, and the radio manager described the frequency of communications interoperability between the system users and state and federal agencies as "often." The system's users also often employ interoperability for mutual aid and task force operations.

The first manager agreed that—

- Encryption is a means of protecting emergency services providers.
- Encryption would improve the security of various agency covert operations.
- Encryption would undermine criminal efforts to evade detection by law enforcement.

The radio manager disagreed that—

- Encryption would prevent the public from receiving information to which they are entitled as taxpayers.

- Encryption would prevent volunteers or off-duty staff from receiving notifications that they are needed.

- Encryption would prevent the news media from keeping the public informed.

- Encryption would impede the public's "right to know."

- Encryption would prevent the public from assuring that their services are being operated for the public good.

Although there are approximately 2,000 users in this public safety communications system, only 300 radios are capable of encrypted communications. His concerns about implementing a fully encrypted communications platform were mainly associated with the efforts required to properly administer an encryption system and the expenses incurred in attaining and maintaining secure keys. Encryption, he stated, increased costs by forcing management to track the individual pieces of communications equipment more closely to assure they were all keyed properly. This same key issue impacted interoperable communications, he believed. This was because of the potential for a lapse in communications due to different segments of users using different keys. Encryption would also be more expensive to acquire, with his equipment supplier quoting a cost of $600 additionally for each radio that was encryption capable. Interoperable communications, he believed, would become much more difficult if encryption were used.

This radio system manager sought a few different means of evading monitoring. These means, he stated, were less expensive and readily available. They included employing enhanced special mobile radio (ESMR) services such as NEXTEL®, commercial radio services, and even family radio service for such varied public safety interests as low-security, short-range needs, or high-security assignments when evading criminal elements using scanners was desirable. These measures had been economical and effective, and allowed ample system services to be available until the new system became operational.

The second radio system manager contacted was responsible for a large public safety communications system serving a town, city, and county agencies around a large city in the Northwest. There are more than 13,000 radio users in this system, which is composed of fire protection, emergency medical, and law enforcement services.

The communications system in place is a combination of trunked digital and analog technology. The system is compliant with TIA/EIA-102 and P25 standards. There are no encryption features in this system, and the radio system manager does not plan to seek encryption in any future system upgrades or replacements. The system's security measures provide for over-the-air rekeying (OTAR) and for inhibiting lost or stolen radio equipment.

Interoperability is a key feature in this communications system. By sharing system resources, there is a constant stream of interoperable communications among local public safety agencies, for daily, mutual aid, and task force radio traffic. While there are no day-to-day communications with state agencies, there is a constant use of interoperability for communications with state agencies involved in mutual aid and task force operations. Occasionally, interoperability is employed for task force operations with federal agencies. This system also includes commercial users, operating under contract with the public safety agencies, including medical transportation services.

The second manager agreed that—

- Encryption would improve the security of user agency's covert operations.

- Encryption would prevent the public from receiving information to which they are entitled as taxpayers.

- Encryption would prevent volunteers and off-duty staff from receiving notifications that they are needed.

- Encryption would prevent the news media from keeping the public informed.

- Encryption would impede the public's "right to know."

- Encryption would prevent the public from assuring their services are being operated for the public good.

The radio manager disagreed that—

- Encryption is a means of protecting emergency services providers.
- Encryption would undermine criminal efforts to evade detection by law enforcement.

Costs and administration were among this radio manager's primary concerns in implementing encryption. They were not his only concerns, however. He stated that the cost for implementing encryption was prohibitive. His estimates for the amount of air time that encryption would be beneficial was "1 percent." With the additional expense involved in buying radio equipment capable of encryption, the return on the investment was too little and the cost too high to justify. His other concern with encryption was that this technology supported an agenda allowing inappropriate use of public safety radio communications by public safety personnel.

This radio system manager believed that the public generally was indifferent about what their public safety agencies were doing on a day-to-day basis. A small segment, though, listened in order to monitor its public services. Encryption would limit public access, and he believed that preventing this minority in our society from monitoring would allow public safety agencies to hide behind their official status to avoid scrutiny. He stated that all public safety radio traffic should be open to reception because the public had a right to know what its tax dollars was supporting and how its public services were being provided. Attempts to prevent this openness would lead to distrust by the public in its public safety agencies.

There were a few circumstances, this radio system manager stated, where encryption would be justified. The circumstances he provided included responses to civil disorder, weapons of mass destruction (WMD) incidents, and narcotics enforcement investigations and operations. Otherwise, he concluded, the public should be able to monitor all public safety radio traffic freely.

The third radio system manager interviewed is responsible for statewide law enforcement communications in an East Coast state. There are approximately 2,500 users in this system, which is a conventional analog radio system. Although this radio manager was familiar with the TIA/EIA-102 and APCO P25, his system is not currently compliant with these standards. It was his intent to implement these standards and Data Encryption Standards (DES) in his next system acquisition.

The current system in this state is in need of security measures. Among the needs this manager identified were voice privacy, encryption, and a means of inhibiting lost or stolen radio equipment.

When asked to characterize the use of interoperable communications on a daily basis, this radio system manager said that interoperability came into play many times each day in his state with local agencies, either for routine law enforcement activities or for task force operations. Sometimes interoperability was employed for day-to-day or a task force operation with federal agencies, but it was seldom important for mutual aid communications with federal or even other state organizations. There were a number of commercial services operating under contract with the state, and day-to-day interoperability was important with these companies.

This manager agreed with each of the statements concerning encryption, except one. He disagreed that encryption would prevent the public from assuring that their services were being operated for the public good.

When asked what concerns this radio system manager had about employing encryption in his communications system, he provided several. First and foremost, he stated, it was costly to implement encryption and it was not clear whether the cost of encryption could be justified. His agency also had prior experience with a particular manufacturer’s provision for security via digital voice privacy. This feature was employed by his agency for executive protective details. Users found that this feature was difficult and cumbersome to use. As a result, this feature was disabled years ago in favor of using plain voice communications, with more care given to the content of messages rather than to whether or not to communicate.

This experience led this radio system manager to decide that if encryption were to be acquired, it would have to be easy for radio users to employ. An additional concern was that any new encryption technology should be easy for his agency to establish and operate on a statewide basis, to allow for rapid deployment of law enforcement resources anywhere and anytime.

His final concern was that encryption might have a negative impact on interoperable communications. The radio manager stated that of the two issues, interoperability was more important in his state than encryption in the delivery of communications services.

The fourth radio system manager is responsible for a statewide public safety communications system that serves law enforcement and fire protection agencies in an upper Midwest state. There are approximately 8,000 system users on the system.

The statewide communications system is trunked digital primarily, but includes a conventional digital mutual aid system. It is a TIA/EIA-102 and P25 compliant system and includes DES. Security measures, in addition to DES, include the ability to inhibit lost or stolen radio equipment. In this system, DES is used primarily for narcotics enforcement activities.

Interoperability is one of the strengths of this system. Day to day, users in the system communicate with Native American tribal and local public safety agencies and sometimes with federal agencies. Interoperable communications are sometimes used for mutual aid involving local and federal agencies. Tribal agencies use a separate system for mutual aid communications. Task force communications are used on a less frequent basis at all levels.

The fourth manager agreed that—

- Encryption is a means of protecting emergency services providers.
- Encryption would improve the security of user agency covert operations.
- Encryption would undermine criminal efforts to evade detection by law enforcement.
- Encryption would prevent the public from receiving information to which they are entitled as taxpayers.
- Encryption would prevent the public from assuring their services are being operated for the public good.

The radio system manager disagreed that—

- Encryption would prevent volunteers or off-duty staff from receiving notifications that they are needed.
- Encryption would prevent the news media from keeping the public informed.
- Encryption would impede the public's "right to know."

This fourth radio system manager expressed few concerns about encryption. He noted that in a large communications system, keeping the OTAR and encryption keys "fresh" or current was a problem. Operating a system with many users could make maintaining encryption difficult.

This radio system manager also noted that the fire service in his state was not using encryption, and that fire service members did not want to use encryption. In fact, he added, the switch from analog to digital communications alone had caused great strife because low-cost radio receivers and scanners were no longer of any use. Because scanning technology for trunked digital systems has not yet been perfected, fire service interests had suffered a gap in communications. This was because, in the past, scanners had been widely employed as a means of alerting volunteers to fire and rescue emergencies. The radio system manager recalled receiving complaints from fire service personnel and even firefighter families expressing their distress that their scanners had become useless.

3.4 Conclusions

Each of the four radio system managers interviewed agreed on one point regarding encryption: they were not aware of any laws, codes, ordinances, or regulations that existed at the local, state, or federal level that would prohibit them from implementing encryption in their communication systems. There were other security issue areas in which all four of the radio system managers agreed:

- They all used some common security technology in their systems.

- They all said that cost was a prohibitive factor in implementing widespread encryption in their radio communications systems.

- They all recognized that managing a fully encrypted radio communications system properly required more effort and maintenance than they were willing to provide.

Although the regulations and laws regarding encryption were written decades ago, it seems that few in the public safety communications arena have followed their development or are familiar with them. This is largely due to the lack of interest in local and state agencies in add encryption to their radio systems. Only the Federal Government has taken the use of encryption to heart by including some level of cryptology in its communications system designs.

Previously used technology, according to anecdotal information gained during the interview process, was expensive, caused a degradation of signal strength and voice quality, and rendered communications systems less effective than when the same systems were used in a clear voice mode. This circumstance, and the stories surrounding it, has caused radio system managers with experience using encryption to disable that portion of their systems, or abandon that security feature in subsequent equipment acquisitions. In turn, these radio system managers have passed their experiences along to other colleagues.

One of the strongest concerns with modern encryption technology is cost. Each radio system manager was able to quote vendor estimates of the cost that would be added to each portable and mobile radio purchased with an encryption feature. These same managers remarked that they were unsure that the additional expense could be justified, with the exception of a few specific circumstances. Even radio system managers with encryption in their current system had a limited number of user radios equipped for encrypted messaging.

Maintaining an encrypted radio communications system was another strong concern. Proper maintenance, including the term “fresh” as referred to previously, included frequent changes of the encryption key to prevent outside interests from successfully de-encrypting radio traffic. Regardless of whether each radio was keyed individually at a key maintenance facility, or OTAR was used, all the managers worried that they would overlook maintaining each user radio in a timely fashion. The managers expressed a concern that someone would be left with a radio that was useless to communicate with other public safety personnel or to call for help and have that message received. This was an especially significant concern when the maintenance issue pertained to interoperability. The radio system managers all indicated that maintaining valid encryption keys might prove too difficult to assure the integrity of communications interoperability. Where the radio system manager was responsible for a statewide agency, there was a concern that maintaining an effective cryptology feature was vital and yet likely impossible due to the size of the system and the number of radio users. In local systems, the radio system manager was confident in believing that different segments of users may be missed when a key was created, modified, or destroyed to assure system security was optimal. All of the managers stated that the costs of maintaining fresh keys and disseminating keys were significant, and perhaps too expensive to justify assigning staff to accomplish this regularly.

The four radio system managers had varied opinions, however, on the value of encryption in their communications systems. The experience of one of the four managers in using a method of scrambling (voice inversion) radio traffic was negative, and had caused him to rethink encryption. Another said that there was no place for encryption in public safety communications because the public does have a right to know what is happening in their communities and what their public safety agencies are doing.

The experiences of the government agencies that switched from analog to digital communications serve well to illustrate that adding more security features to replacement or upgraded communications systems eliminates a number of security risks but creates another set of problems.

One conclusion is clear from the research—in this country the public's perceived "right to know" is influential in shaping policy regarding communications system access. Where government has recognized this, efforts have been made to provide for this access in a responsible and controlled manner that balances the "right to know" with the need to protect confidential investigations and operations. Where government failed to acknowledge this issue, legal challenges have been threatened. Ultimately in these instances, government successfully worked with the media to stave off these challenges. None of the actions threatened has made the transition into the justice system, so no long-term conclusion about the weight of the public's "right to know" can be discerned. As more public safety agencies systems work to replace legacy systems and build new systems that incorporate security measures, new challenges to these measures can be anticipated. What seems clear is that as long as state and local government administrators recognize these potential challenges and keep clear lines of communications with their communities, a realistic solution to this issue can usually be found.

4. FISCAL CONSIDERATIONS

4.1 Fiscal Issues

The planning, acquisition, and implementation of a new communications system for a public safety entity can be a complex and monumental undertaking. There are many significant decisions to make and a variety of different feature and function options to be considered in today's new generation voice communications systems. Many of these decision points may have far-reaching effects on the finally delivered systems. One of these complicated decisions for communications systems planners, public safety officials, and governing bodies focuses on the acquisition and deployment of encryption technologies within a new system. Depending on the type of communication system, the number of subscriber units, and the level and degree of encryption to be deployed, agencies may realize substantial additional costs.

Therefore, public safety officials and their governing bodies must contemplate the inclusion of encryption services while giving due consideration to the user agencies' operations, requirements, interoperability, and available project funding.

In many cases, state and local governmental agencies have decided against the use of encryption technologies within their new communications systems for some of the following reasons—

- Cost incurred for infrastructure and subscriber portable and mobile units encryption components are high.
- Encryption services would be used by a select group of personnel or in selected assignments or functions, and the return on investment (ROI) is very low.
- Limited funding is available to acquire the baseline system, and encryption is considered a "bell" or "whistle" or enhanced feature.
- Additional basic or required capabilities or equipment can be acquired if encryption services are not included.
- Encryption capabilities can be added in the future should conditions and operations warrant and funding permit.
- Other opportunities or communications capabilities can be used if secure communications are required.

4.2 Technological Advances

Consistent with other advances in technology, encryption services for voice radio systems have continued to evolve. The convergence of digital capabilities into voice radio systems has actually provided a better foundation to support emerging encryption technologies. Today, much of the digital encryption technology has evolved from the information technology (IT) industry and is incorporated in radio system offerings from various vendors.

Encryption has been and continues to be available for conventional and trunked systems as well as systems supporting older analog and the newest digital protocols. Each of the major system manufacturers offers encryption components for their respective systems. In addition, several vendors produce after-market components that are available for installation into base station repeaters and subscriber mobile and portable equipment.

Normally, as the end of the life cycle of current and legacy public safety radio systems nears, manufacturers will routinely discontinue support of certain equipment including encryption technologies. Presently, one of the major system manufacturers has indicated that encryption services for its legacy analog systems will be discontinued. Owners of these systems who want to add encryption features must replace their infrastructures along with the subscriber equipment that will support current digital radio and encryption standards. This migration translates into a significant overall cost that may reach into the millions of dollars in even small-to medium-sized systems.

4.3 Cost to Implement

The cost to implement encryption capabilities on a given voice communications system may vary widely. Costs may be affected by—

- System design—single site, multi-site, multicast, or simulcast
- Degree or level of encryption desired—subscriber only based or “end-to-end”
- Number of subscriber units to be “encryption capable”
- Required infrastructure enhancements
- OTAR capable or manual key programming
- System type —conventional or trunking
- Transmission protocol—digital, analog, or both
- When encryption is implemented—initially or after implementation
- Interoperability.

4.3.1 New System Development Cost

Table 1 lists the estimated costs agencies contemplating deployment of encryption services can expect from the major systems vendors for encryption equipment and services. The costs presented are averages.

Table 1
Estimated Costs—Encryption Equipment and Services (Major Vendors)

Equipment/Service	Average Cost	Comments
Subscriber unit digital encryption module	$700–$1,000/unit	Dependent on vendor and equipment models
Key loader	$2,000–$3,500	Quantity of two minimum is recommended for all systems
Training—Technicians/Administrators	2 days—$1,000–$1,500/day/ person	Recommend minimum of two agency participants
Training—Users	30 minutes to 1 hour—$100–$200 (10 to 20 per class)	May vary if in-house training is utilized
Component installation for existing subscriber equipment	$75.00–$100.00/unit	Equipment must have been originally capable of supporting encryption
System infrastructure review and tuning for encryption	$150—$250/hour	
Console digital interface units	$2,200–$3,000/per channel	Allow dispatcher consoles to encrypt/decrypt transmission
Over-the-air-rekeying (OTAR) software	Varies	This cost could be as high as $50,000 depending on system configuration
Personal computer for OTAR and key management	$2,500–$3,500	Standalone computer only needed if OTAR is used

4.3.2 Aftermarket Implementation

As previously stated, encryption components may also be available from third-party or aftermarket suppliers. These vendors provide encryption modules for installation into various models of subscriber equipment and some base station equipment. Equipment to support the encryption services is also available. Table 2 lists the average costs for purchase from these sources.

Table 2
Estimated Costs—Encryption Equipment and Services (Third Party/Aftermarket)

Equipment/Service	Average Cost	Comments
Encryption module	$75–$700/unit	Dependent on vendor and equipment models and the level of encryption [11]desired
Key loader	$1,200–$2,500	Quantity of two minimum is recommend for all systems
Training—On-site technical services	$1,000–$1,500/day/ person	Recommend minimum of two agency participants
Training—In-house at vendor location	$500/person/session	

[11] Several after-market vendors offer different levels of proprietary encryption. Several of these levels of capability are based on voice frequency inversion, "voice scrambling," or code changing/hopping. These techniques do not actual digitize the voice content. In the higher offered levels, actual DES is offered.

Equipment/Service	Average Cost	Comments
OTAR software	$100–$1,000	
Personal computer for OTAR and key management	$2,500–$3,500	

Agencies contemplating use of third-party after-market products should ensure compatibility with existing subscriber and infrastructure equipment. In addition, it is very important to review existing warranty and service agreement contractual requirements. The installation or use of third-party components within existing products may adversely affect warranty and service level agreements.

Agencies should also be aware that potential additional costs might arise if the system infrastructure troubleshooting must occur to permit the proper operation of the encryption components. Performance-based contracts that provide sufficient provisions to protect the public safety agency from these unexpected cost overruns are recommended.

As another potential alternative to replacement of entire trunking system infrastructures, several agencies have opted to deploy single-channel conventional digital systems with encryption capabilities to cover their operational service area. Depending on the existing systems, complexities of the system configuration, and opportunities for site sharing, this approach may be a viable alternative for some agencies. In addition to the base station equipment, subscriber equipment is purchased or upgraded to support the existing analog trunking system and the new digital encrypted conventional system. Table 3 lists the estimated cost for this type of alternative.

Table 3
Estimated Costs—Single-Channel Conventional Digital System with Encryption

Equipment	Estimated Cost	Comments
Base station package	$50,000	Includes installation, high-gain base antenna, line kit, software, optimization, etc
Project 25 compliant subscriber	$2,000 to $4.500	Mobile or portable with DES encryption. Cost varies by manufacturer and features
Key loader with accessories	$3,500 each	Recommend quantity of two minimum

It is important for agencies to recognize that although it is technically possible to implement encryption after the initial deployment of a new system, this approach would certainly incur additional costs. Vendors estimate these costs at from 10%–30% of the original system cost based on the system type and configuration. The more complex the communications system, the more the costly it is to deploy encryption features. Costs are also associated with installation of cryptologic modules within mobile and portable subscriber equipment and reprogramming of the individual radios to support encryption capabilities.

Potentially, additional tuning of the system infrastructure may also be required to ensure that the encryption components work appropriately within the system. This is especially true in systems employing multiple sites and critical site timing. This manipulation of the infrastructure may result in some degree of service interruptions or difficulties while the system-level components are verified for correct operation. If "end-to-end" encryption services are selected, additional encryption devices may be required for consoles, microwave or telephone support circuits, or other communications paths that carry the voice audio. Cost associated with these components cannot be readily estimated because they are vendor, system, and configuration dependant.

Agencies should also be aware that additional public safety personnel time and radio technician time would be expended to upgrade each mobile and portable radio to support encryption in the system. A degree of training will also be required for all personnel using encryption services, as well as those responsible for encryption key loading and management.

According to public safety agencies that currently use or have implemented encryption "after-the-fact" and the vendor community, the decision to include and deploy encryption services should be made ***before*** the initial deployment of any new system. This is especially true of more complex simulcast and/or multicast systems. If included in the initial system implementation, all infrastructure and subscriber equipment can be ordered with encryption capabilities already configured. Training can be included with other system and user training more efficiently. Agencies may also be able to acquire better pricing for encryption components and services as a part of the overall system purchase than might be available after to implementation.

It is of paramount importance that agencies work closely with their systems vendor to ensure that appropriate encryption equipment and services are selected for their system configuration consistent with the user agency requirements for secure voice transmissions. A comprehensive acceptance testing plan should be prepared by the agency and the vendor to ensure that encryption capable equipment continues to function optimally in both encrypted and clear modes of operation.

5. SUMMARY

The consideration and incorporation of encryption capabilities in state and local public safety communications systems presents an entirely new set of issues and challenges. While some type of encryption capabilities have been available to protect radio transmissions since the 1930s, it has only been in the past decade or so that the Nation's public safety community has begun serious scrutiny of the various opportunities. The federal law enforcement community has embraced this technology, but the state and local public safety community has been reluctant to implement it for various reasons. These reasons fall into three categories:

- Legal and regulatory issues
- Public safety operational issues
- Fiscal considerations.

In the legal and regulatory area, no known federal or state laws or regulations specifically prohibit or require critical public safety communications to be encrypted or remain "in the clear." Several cases have been considered by the courts regarding the "public's right to know" concept, but no single definitive ruling gives clear guidance on this issue. It is generally accepted that if a radio message is broadcast in clear voice, then it is public information. If public safety wants to protect this information, security measures such as encryption can be used, which may make interception of the information illegal. However, by using encryption, these agencies may be vulnerable to legal action under the FOIA or Privacy Act, or subject to constitutional challenges covered by the First and/or Fourteenth Amendments from members of the news media or the general public. A legal test of the concept of the "public's right to know" versus an individual's expectation of privacy has not yet occurred. There have been no definitive rulings or findings regarding the legality or legitimacy of the use of encryption technologies by public safety agencies or the potential of an expectation of privacy by these agencies or their member personnel. All of these potential legal issues and challenges remain obscure.

There are also Presidential Decision Directives that appear to imply that the use of encryption should be required for public safety communications, but at the same time, they are vague enough to allow for different interpretations by different agencies and the legal community. This area continues to be undefined, and potential risks are present.

In the operational arena, the response to encryption is even more confusing. Although most state and local law enforcement agencies support the use of encryption for some communications activities, the fire and emergency medical community remains firmly against its use with the single exception of patient information, which has long-standing confidentiality requirements. Many fire/EMS agencies have concerns that encryption services may hamper communications interoperability and their ability to notify volunteers, off-duty staff, and their local communities of incidents without the purchase of costly equipment. Furthermore, some believe that there is a distinct potential for missed communications in fully encrypted systems due to missed key updates of portable or mobile radio equipment.

Radio system managers who were interviewed could not agree on the need for the use of encryption for several reasons—all related serious concerns about the additional cost, additional equipment required, the additional work of managing an encrypted system, and the relatively low return on investment that encryption components may generate. However, all agreed that if a technology such as encryption was being planned for a system, there needed to be a close dialog with local news media and community groups to try to avert the possibility of potential legal actions.

The area of greatest impact regarding the use of encryption at the state and local level appears to be adequate available funding. The implementation of encryption is expensive, costing from $700–$1,000 per typical digital radio subscriber unit. An effective encryption key management program is also needed, which again adds additional labor, equipment, and facility costs. Most public safety agencies' communications budgets are strapped for funding and barely provide enough for basic services. In these situations, encryption is seen as a "bells and whistles" type feature and is often removed from a new system design in favor of purchasing additional baseline radios and system infrastructure equipment. Given the opportunity to provide additional communication resources or encryption, the majority of agencies indicate that they would forego encryption. The perceived ROI that would be realized from using encryption is negligible.

Agencies desiring to pursue the use of encryption should recognize that the cost could be better controlled if these plans were made in the initial system planning and design. Implementing encryption on existing systems is usually more expensive and, in some cases, may not be possible because manufacturers are no longer supporting some of the legacy encryption systems used on older analog systems.

If the state and local public safety communities are expected to embrace and further the use of encryption technologies, several issues must be addressed:

- Funding—New sources of funding must be proposed or identified that will allow state and local public safety agencies the opportunity to plan for and implement security measures to protect their communications systems and messages.

- Standards Development—The public safety community—local, state, and federal agencies—as well as vendors must become actively involved in the development and implementation of advanced encryption standards within their respective equipment. Only by the development and enforcement of standards in these areas can the ability of equipment and agencies to interoperate be assured.

- Legal and Regulatory—Governmental agencies at all levels must closely monitor this area to ensure that public safety's ability to protect critical communications is not diminished or ultimately unduly restricted. Although not all in this sector agree on the need for widespread use of encryption, the loss of this ability could endanger our Nation's citizens, its public safety personnel, and its ability to successfully complete its critical responsibilities and missions. The public safety community may consider a proactive initiative to encourage the FCC, the Congress, and other regulatory authorities to establish effective public policy regarding the proper balance of the "public's right to know" and public safety's ability to protect sensitive critical communications and information.

- Education—Groups such as the PSWN Program must continue to provide up-to-date information to the public safety community so that they fully understand the potential threats they face and how these threats may be mitigated. This education must also include law-making and regulatory groups, the news media, and the general public so they can understand the unique situation of the public safety community and the dilemmas faced in trying to balance the expectations of privacy with the free flow of information.

The issues and impediments that the public safety community faces in trying to secure its communications are many and complex. By applying the lessons learned from past successes and failures, and proactively addressing the issues identified, the goal of secure communications that serve all involved is realistic and attainable.

6. ADDENDUM

6.1 Impact of the Terrorist Attacks on Opinions Regarding Communications Security and Encryption

On September 11, 2001, terrorist attacks were launched along the Eastern seaboard of the United States. Thousands of people died and billions of dollars in economic damage resulted due to property losses, business disruptions, and unemployment. Additionally, the attacks of September 11 killed more Americans than on any day since the Battle of Antietam during the U.S. Civil War. More American firefighters, police officers, and other public safety personnel were killed in the line of duty that day than on any other day at any time in recorded history.

The response, mitigation, and recovery activities following these attacks have been unprecedented in American society. Security for public facilities and the general public infrastructure is more visible and intense than at any time since World War II. This heightened level of security, in many ways, is due to advances in the use of technology for security and protective measures. Public safety agencies at the local, state, federal, and tribal levels of government all were called to duty as a result of the terrorist attacks of September 11. Many of these agencies provided a response to the scenes of the attacks in New York, Virginia, and Pennsylvania. Many public safety and protection agencies were impacted because they were required to react within their jurisdictions and provide a heighten level of security and protective services to minimize or prevent further terrorist actions.

Because of the events of September 11 and the ongoing activities at various levels of government to increase the Nation's protective stance, the PSWN Program re-interviewed the original contributors to this report to learn whether their viewpoints on the use of encryption in public safety communications had been influenced. They were also asked whether their agencies were addressing security differently and if so, how.

6.2 Encryption and Security

The PSWN Program originally interviewed four radio system managers. This diverse group included—

- The radio manager for a countywide system serving more than 2,000 public safety users, including town, city, county, and regional police officers, sheriffs, and the largest fire and rescue organization in the state, located in a large mid-Atlantic county.

- The radio manager for a regional system surrounding a large metropolitan city in the Northwest that serves more than 14,000 public safety and general government users at all levels of government.

- The radio manager for law enforcement communications for a state police agency with more than 2,500 users in an East Coast state.

- The radio manager for a statewide public safety communications system that serves law enforcement, fire protection, emergency medical, and general government services in an upper Midwest state.

The second series of interviews found that these radio managers had not substantially changed their points of view regarding encryption. One manager had narrowed his views regarding the use of encryption to preventing the media and the public from gaining information and had doubts that encryption would prevent volunteers or off-duty staff from being notified of the need to report for duty. "There are other ways to accomplish these things," he said, referring to changes in paging technology that are available and the widespread use of this technology to respond to the attacks of September 11. In this manager's state, he acknowledged that the news media had developed alternatives for electronic news-gathering (ENG) in response to digital trunking in public safety communications systems. He further stated that things were not the same elsewhere and that colleagues continued to wrestle with issues of media access.

The other state system radio manager reported that a television station had been refused "real-time" access to the digital trunking system. The station had been experiencing gaps in its ENG and sought "receive-only" access via a subscriber unit to the statewide system. The system's advisory board refused the request, and now the television station is awaiting the arrival of digital trunk-tracking scanners, expected by late 2002, as a solution.

One of the local radio system manager's views remained unchanged regarding encryption. He reported that in neighboring jurisdictions with encryption-capable communications systems, discussions with his counterparts revealed that none of them had been using encryption consistently prior to September 11 and that none of them had plans to implement consistent use of encryption since the attacks. While surprised by their decisions not to change their practices, this radio manager wondered how important it was to add encryption to his system if his peers who already had encryption were not using it. His communications system did not have encryption capabilities, and since it was not a widely used feature in his region, then he could not see the value in expending considerable resources to expedite the implementation of the feature.

Following the September 11 attacks, a general security analysis was initiated by all of the radio managers' governmental agencies. All found some need to improve protection measures for their physical plants and infrastructure components, and all had taken steps to do so.

One local radio manager expressed his opinion that future security concerns about radio traffic were less important than concerns about protecting systems' infrastructure. He believed that criminal elements might monitor and use radio traffic for their enterprises—which, in fact, had been done in his area. He indicated that during a recent period of civil disobedience, public safety officials learned that their analog radio traffic was monitored and re-broadcast over the Internet. The agencies involved switched to digital channels within the system for the remainder of their operations for the incident. In his opinion, terrorists, on the other hand, would be more likely to attack the physical plant for public safety communications systems. Infrastructure protection was where he believed investment in greater security should be made. It was also where he believed an appreciable, visible return for that investment was probable.

One of the local radio managers also offered the following reasons why his opinions had not wavered after the terrorist attacks. “The attacks of September 11 didn’t change my opinions about encryption or communications security,” he stated, “and the attacks did not change the work that my agency is doing to prepare for the new communications system. It’s really the work of the PSWN Program that influenced my opinions, and the work we are doing for our system. The PSWN Program did that almost 2 years before the September 11 attacks.”

“If anything,” he continued, “the attacks of September 11 validated the attention and guidance that the PSWN Program has given to communications security.” The radio manager went on to note that PSWN Program publications on the topic of security have depth and value. “My agency has certainly used [these publications] in planning for its next communications system,” he concluded.

6.3 Conclusion

The attacks of September 11 motivated governments at all levels to review security features and practices for their entire operations. The impact on radio systems has been to improve measures for physical and infrastructure security. The case for improved security in communications and system architecture through the use of encryption technologies still has not been made. Expense, coupled with the concern that less-than-ideal management resources and practices are available, remain significant reasons why radio system managers find it prohibitive to move encryption into their systems for consistently secured radio traffic.

Although interviews of four radio system managers cannot be regarded as statistically representative of the public safety industry, conclusions can be drawn based on the views of those interviewees contacted. There are three primary conclusions to be drawn. Local and state radio managers will not be convinced that they can afford the resources required to acquire, implement, and maintain encryption in their systems until the following conditions are met—

1. The cost to acquire and support encryption technologies decreases and a reasonable return on investment can be identified.

2. Key management can be easily accomplished.

3. Radio managers can be assured that users will not be adversely impacted by the management and maintenance required for encrypted radio systems.

Digital trunked system scanners will eventually become prevalent. For now, radio managers are enjoying the benefits of digital trunking technology as a means of providing more private but unsecured voice communications. When this new scanning technology undermines that level of comfort, managers may consider encryption more seriously for securing their users' critical radio traffic, but only if it is affordable and manageable from their viewpoints.