PUBLIC SAFETY PSWN PROGRAM WIRELESS NETWORK

PUBLIC SAFETY WIRELESS NETWORK

Achieving Interoperability through Cooperation and Coordination

For years, public safety agencies have worked to ensure the basic security and integrity of their communications networks. Historically the focus has been on physical security at communications facilities and the encryption of transmissions to protect sensitive information. The use of digital technology, the interconnection of once stand-alone networks, and the increased threat of domestic malfeasance and terrorism have ushered in a new era for systems security. Public safety agencies, like the owners and operators of other critical infrastructures, must take evermore sophisticated steps to safeguard their communications systems from both physical and cyber threats.

These and other considerations make the security environment for public safety communications a growing challenge. In an effort to raise awareness about these issues and to suggest some possible solutions, the PSWN program has developed this guide. I recommend it to you in hopes that it be a catalyst for improving the systems security of public safety communications networks throughout the Nation. I would also like to thank those colleagues of mine on the PSWN Executive Committee who contributed to the development of this guide and endorsed its contents. Special thanks go to the members of the PSWN program's Security Integrated Program Team who dedicated time and effort to complete this guide.

Sincerely,

Steven J. Proctor

Mr. Steven Proctor
Executive Vice-Chair, PSWN Executive Committee, and
Executive Director, Utah Communications Agency Network

About The PSWN Executive Committee

The PSWN Executive Committee is comprised of senior-level executives from local, state, and federal public safety agencies from across the country. Members have proven expertise or accomplishments in the field of law enforcement, fire and rescue, emergency medical services, public safety communications and information technology. The objectives of the committee are to raise awareness on the communications difficulties encountered by public safety personnel and to provide program guidance to the PSWN program as it works to achieve interoperable public safety communications.

PUBLIC SAFETY PSWN PROGRAM WIRELESS NETWORK

This guide was prepared by the Public Safety Wireless Network (PSWN) program. This program is a joint initiative of the Department of Justice and the Department of the Treasury. For more information, visit the web site at www.pswn.gov or call 800.565.PSWN.

PUBLIC SAFETY

Communications Security Awareness Guide

Imagine for a moment…police officers and agents approaching the front and rear of a residence used as a major drug distribution center. Imagine also…known drug felons lying-in-wait inside the residence because they have been listening in on the communications to plan and carry out the drug raid. As a result, the suspects inside are well-informed and well-prepared for the ensuing raid. The information that these suspects possess can be measured in lives.

The protection of public safety communications is often essential for successful completion of public safety operations. Compromise of critical public safety information also can place valiant public safety officers at great risk. Secure public safety communications, including those of fire and emergency medical services, are needed to protect public safety officials and to support mission accomplishment. The key components of secure public safety communications are secure facilities and networks, reliable back-up systems, secure transmissions and constant security awareness.

Anyone who works in an office is well aware that when the phones are down, the ability to accomplish work is limited. So imagine the threat to life and property when public safety officials cannot do their job because of a major disruption in their essential communications systems or when their communications are compromised. Secure

Hacker disrupts service at airport

Business Wire—March 19, 1998

At approximately 9:00 a.m., [a] juvenile computer hacker intentionally, and without authorization, accessed the [phone] system servicing the Worcester Airport…Public health and safety were threatened by the outage which resulted in the loss of telephone service [to the] FAA tower at the Worcester Airport, to the Worcester Airport Fire Department, and to other related concerns such as airport security, the weather service, and various private airfreight companies. Further, as a result of the outage, both the main radio transmitter…and a circuit which enables aircraft to send a signal to activate the runway lights on approach were not operational for this same period of time.

facilities and networks, along with reliable backup capabilities, are vital for public safety officials to perform their jobs safely and effectively at all times.

Increasingly, public safety agencies need to address, head-on, the security of their communications systems. Unsecured systems leave our public safety officials vulnerable and increase the risks to the lives and property of the citizens they are working to protect.

What Is Communications Systems Security?

Communications systems security is the process of developing and implementing specific plans, policies, and procedures to secure public safety communications systems from possible risks and malicious actions. Evaluating and implementing security plans, policies, and procedures is needed to mitigate risks to critical public safety communications systems. These security risks are intentional or unintentional actions taken against a system that could result in the modification, disclosure, or destruction of sensitive or private information. These actions can degrade or fully disable system operations. Communications systems security generally includes four components—physical security, network security, communications security, and administrative security. The design, operation, and maintenance of public safety communications systems, including private radio networks, should address each of these components.

Physical security includes the protection of all facilities where communications system components are housed. This may include the communications center, remote tower sites, and maintenance facilities, as well as the communications equipment itself. Equipment must be secured at all times, including while it is in use, while it is being transported for maintenance purposes, and while it is in the maintenance cycle.

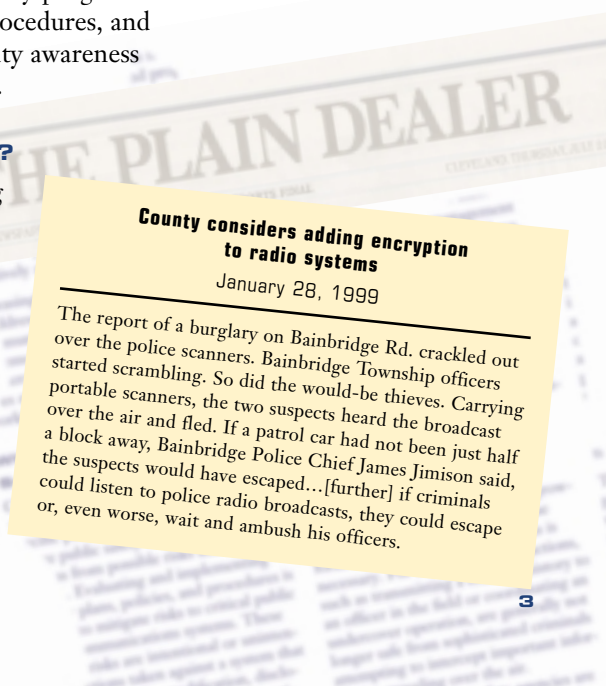
Network security involves the protection of the systems hardware, software, and associated interfaces. Common network security requirements include maintaining user accounts, controlling passwords and system access, performing routine system audits, and removing unnecessary sensitive information from the system.

Communications security relates to those measures taken to ensure the confidentiality and integrity of information transmitted over the airwaves. This includes the use of encryption, the management and reprogramming of encryption keys, and the safeguarding of key codes and software.

Administrative security involves the use of procedural controls to ensure the confidentiality, integrity, and availability of communications systems. An administrative security program would include security plans, procedures, and documentation; on-going security awareness training; and personnel security.

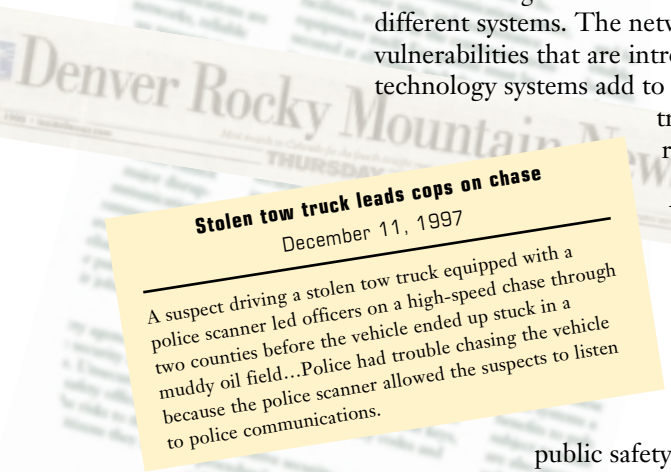
What Is The Problem?

Public safety agencies are facing a growing number of occasions when some form of protected communications is necessary. For example, routine actions, such as transmitting a criminal history to an officer in the field or coordinating an undercover operation, are generally not safe from sophisticated criminals attempting to intercept important information



traveling over the air. Additionally, public safety agencies are facing an ever-increasing number of threats, such as coordinated terrorist attacks to their physical communications infrastructure and remote attacks to their computer-based systems.

Many public safety agencies are also upgrading or replacing their private radio networks. These systems are evolving from stand-alone, analog, voice-only systems to more sophisticated networks. These new networks rely on digital, computer-based technology; support the transmission of voice, data, and video; and have underlying architectures that enable sharing and interconnection between different systems. The network-related security vulnerabilities that are introduced in the newer technology systems add to a considerable set of traditional threats that remain in existing systems.



Additionally, new and upgraded systems are becoming less reliant on proprietary technology and are being developed using common standards. These standards allow public safety communications systems to interoperate, and consequently result in more points of interconnection to other types of communications or remote data networks.

Although these advanced communications systems are providing significant benefits to public safety, they remain subject to traditional security threats and are also more susceptible to new security vulnerabilities. Some agencies are familiar with traditional threats such as radio frequency jamming, physical attacks, and impersonation, unfortunately they generally do not have strategies, or the financial resources, to address them. Agencies are largely unfamiliar with new computer-based threats to their communications systems. Specific training to raise security awareness of these new threats and to identify the necessary risk-mitigation strategies is not available.

The evolution toward automated, computer-controlled communications systems makes the threat of a system hacker more pressing. Depending on the system's features, hackers may infiltrate the system and reprogram radios, change security keys, or reassign talkgroups to different channels. Unsecured systems allow hackers to gain access through a variety of illicit hacking methods such as dialing phone numbers in search of modem tones to access a network and randomly guessing user passwords. Further, public safety agencies are not adequately incorporating security designs into their systems because of limited awareness of these new threats or because of funding limitations.

What Has Been Done?

In the past, the federal law enforcement community has relied primarily on encryption for the security of its voice communications. Some state agencies have also relied on encryption for voice communications security. Encryption technology is mature and the vendor community generally provides encryption features in their product offerings. However, encryption addresses only one aspect of communications systems security and does not necessarily mitigate new, computer-based threats.

In 1996, the security of certain networked systems became a more prominent national issue. The systems of concern included those typically identified as the core infrastructure for the Nation. In particular, The President identified certain

national infrastructures as so important to the United States that an interruption in their service would have a severe impact on the security of the country. The President went on to create a policy stressing the need to protect these infrastructures from physical, electronic, radio frequency, and computer attacks. Emergency services, including police, fire, and medical services, were identified as critical infrastructures.

Vice-President Gore's National Partnership for Reinventing Government (NPRG) also included the idea of communications security for public safety wireless systems in its reports on more efficient and cost-effective government services. An action item contained in the NPRG report *Access America* recommended security be included in all public safety communications systems. In particular, the NPRG action recommended that experts work with the public safety community and industry to define security guidelines, standards, and procedures for public safety communications.

The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63

May 1998

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include…emergency services, both government and private…As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities… Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Since 1996, the Public Safety Wireless Network (PSWN) program has been working with the local, state, and federal public safety community to address the NPRG action and other security issues. Specifically, the program is raising the community's awareness regarding many security issues and threats facing public safety communications systems. The program has also helped public safety agencies better articulate their systems security requirements and is developing generic plans and policies to address many current and future security threats.

What Needs To Be Done?

Although there has been renewed focus on security issues in recent years, the majority of public safety communications systems in the United States are not undergoing any form of security assurance process. There must be significant coordination between leaders from all levels of government and public safety officials to create effective security solutions for public safety communications.

Governmental leaders need to understand the potential security threats and risks associated with evolving public safety communications systems. These leaders can ensure adequate funding is available to secure existing systems and strive to fund only those systems for which security concerns have been addressed.

Public safety agencies must incorporate security measures into their existing systems to the greatest extent possible. As new systems are designed and implemented, agencies should take a life-cycle approach to building security into their systems. This includes security requirements, risk assessments, security tests and evaluation, and security training. Public safety agencies need to understand that prudent systems planning requires the incorporation of appropriate physical and computer security measures into new systems.

For the life-cycle approach to be successful, security considerations must be given priority in other areas. For example, standards associations, vendors, and the public safety community must work together to develop and adopt overarching security standards,

procedures, and guidelines. Equipment providers and systems integrators must in turn incorporate these stipulations into their product and service offerings. Public safety agencies must include security specifications as a part of their requests for proposals when pursuing a new system implementation.

Why Does It Matter?

The security of our Nation's public safety communications infrastructure is an issue that affects us all. Our public safety officers must have secure communications to enable them to protect their lives and the lives of citizens. Additionally, the Nation's communications systems must be protected from destruction and intrusions that may lead to wide-ranging disasters. Measures must be taken to ensure the security of these systems so public safety agencies can swiftly and efficiently carry out their critical activities.

For Additional Information

Digital Land Mobile Radio Security Problem Statement

This problem statement highlights emerging security issues associated with evolving public safety radio communications systems. This narrative addresses the vital need for security from an infrastructure protection perspective, explains the cause of new security threats and vulnerabilities, and highlights the security challenges that face the public safety community.

Digital Land Mobile Radio System Security Guidelines Recommendations

This document describes recommended radio system security guidelines, including industry best security practices. These guidelines can be applied to the design, implementation, and operation of digital land mobile radio systems.

Security Field Data Collection Reports

These reports summarize the findings and candidate recommendations developed from the PSWN program's security field data collection visits to local, county, and state public safety agencies. These reports help increase the understanding of security issues associated with evolving public safety communications infrastructures and identify best security practices that decrease risks to public safety communications systems.

Presidential Decision Directive 63

This directive stipulates that emergency services communications be protected from physical and cyber threats. For more detailed information on Presidential Decision Directive 63, contact the Critical Infrastructure Assurance Office at 703-696-9395. For copies of the White Paper on Critical Infrastructure Protection visit http://131.84.1.84/6263summary.html.

These and other publications are available from the PSWN Program by visiting the web site at http://www.pswn.gov or calling 800-565-PSWN.