



Wireless Communications Security

Awareness Guide



Homeland
Security

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 consequences of unsecure communications can be measured in lives.

The protection of emergency response communications is often essential for successful execution of emergency response operations. Compromise of this critical information can place emergency response officers at great risk. Secure communications for police, fire, and emergency medical services (EMS) responders are needed to protect emergency responders and to support mission accomplishment. The key components of secure emergency response communications are secure facilities and networks, reliable backup systems, secure transmissions, and constant security awareness.

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

Secure facilities and networks, along with reliable backup capabilities, are vital for emergency responders to perform their jobs safely and effectively at all times.

Increasingly, emergency response agencies need to address, head on, the security of their communications systems. Unsecured systems leave

Hacker Breaks Into Emergency Communications System in Maryland
November 30, 2005

A computer hacker broke into the Prince George's County emergency communications system and transmitted a false emergency request. Fortunately, a fire chief recognized it as a false alarm. Still, responders at Station 9 firehouse were very concerned that the breach could have sent firefighters on an errant call, preventing someone else from receiving the emergency help really needed.



these responders vulnerable and increase the risks to the lives and property of the citizens they are working to protect.

What Is Communications System Security?

Communications system security is the process of developing and executing specific plans, policies, and procedures to secure emergency response communications systems from possible risks and malicious actions. Evaluating and implementing security plans, policies, and procedures is needed to mitigate risks to these critical communications systems. These security risks involve 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 emergency response 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
- while it is being maintained

Network security involves the protection of the system's hardware, software, and associated interfaces. Common network security requirements include maintaining user accounts, controlling passwords and system access, and performing routine system audits. Firewalls, anti-virus software,

and intrusion detection programs also play an important role in maintaining network security.

Communications security relates to 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, key loaders, and related 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, ongoing security awareness training, and personnel security.

What Is The Problem?

Emergency response 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. In addition, emergency response agencies are facing an ever-increasing number of malicious acts, such as coordinated terrorist attacks on physical communications infrastructure and remote attacks to computer-based systems.

Another area of concern stems from the fact that many emergency response agencies are 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 and support the transmission of voice, data, and video. They also have underlying architectures that enable data sharing and interconnection between different systems. The

Interference over Police Communications System in Wisconsin March 2004

A former University of Wisconsin–Madison graduate student was arrested after Madison Emergency Radio System technicians traced the location of a transmission interfering with Madison Police Department (MPD) radio frequencies to his apartment. Prosecutors believe that the transmission was retaliation against the MPD for convicting the suspect of speeding earlier that day. The MPD also complained of an incessant tone transmission that had interfered with its portable radios two weeks earlier. Police department radio technicians later traced that transmission back to the same suspect's apartment.



newer technology systems introduce network-related security vulnerabilities on top of the considerable set of traditional systems threats.

The devastation caused by the September 11, 2001 terrorist attacks and by natural disasters, such as Hurricane Katrina, has raised several additional concerns about emergency response communications. The need for interoperability has become an increased priority. As new and upgraded systems are developed to meet this need, more points of interconnection to other types of communications or remote data networks occur, introducing a new host of security risks. Interoperability solutions themselves, including mobile devices, or on-scene audio switches, can negate traditional security methods and present new problems to the safety of an emergency responder network.

Multiple Burglaries in Virginia

July 2003

Four Stafford County teenagers operated a “highly organized” commercial burglary ring, committing more than 17 break-ins within the year. The teenagers pre-planned each burglary and evaded capture by using police scanners to listen in on the police communications and positions. They were finally caught after the police received information naming the suspects.

Although advanced communications systems are providing significant benefits to the emergency response community, 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 monitoring of unencrypted traffic, radio frequency jamming, physical attacks, and impersonation. Unfortunately, they generally do not have strategies, or the financial resources, to address them. Moreover, 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 necessary risk-mitigation strategies is not widely available.

The evolution toward automated, computer-controlled communications systems heightens threats from system hackers. As new services and access to data become available, officials need to consider the additional vulnerabilities to systems. Depending on the system’s features, hackers may infiltrate the system by introducing a virus, disabling



the system, or obtaining confidential information. Unsecured systems allow hackers to gain access through a variety of illicit methods such as dialing telephone numbers in search of modem tones to access a network and randomly guessing user passwords. At the same time, emergency response agencies are not adequately incorporating security designs into their systems because of funding limits and a lack of resource allocations.

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 its product offerings. In November 2001, the National Institute of Standards and Technology (NIST) accepted and authorized the Federal Information Processing Standard (FIPS) 197 for the Advanced Encryption Standard (AES). This provides a more robust encryption algorithm. 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, President Clinton identified certain national infrastructures as so important to the United States that an interruption in their service would severely affect the security of the country. Through Presidential Decision Directive (PDD) 63, Clinton created a policy stressing the need to protect these infrastructures from physical, electronic, radio frequency, and computer attacks.

The Bush Administration's Policy on Critical Infrastructure: Homeland Security Presidential Directive (HSPD-7)

December 2003

"This directive establishes a national policy for Federal departments and agencies to identify and develop processes and technologies to protect all critical infrastructure and key resources of government and economic sectors . . . While it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the country, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks to the same suspect's apartment.



Emergency services, including police, fire response, and EMS, were identified as critical infrastructures.

Following the terrorist attacks of September 11, 2001, President George W. Bush revisited the importance of the Nation's critical infrastructure by issuing Homeland Security Presidential Directive 7. This directive, which supersedes PDD 63, strengthens the national policy for securing the country's critical infrastructure.

In addition, the Department of Homeland Security continues to raise the community's awareness on many security issues and threats facing emergency response communications systems.

What Needs To Be Done?

Although there has been renewed focus on security issues in recent years, the majority of emergency response communications systems in the United States do not have any form of security assurance process. Leaders from all levels of government, as well as emergency response officials, need to elevate security awareness and allocate resources within procedures and guidelines. Equipment providers and systems integrators must in turn incorporate these stipulations into their product and service offerings. Emergency response agencies must include security specifications as a part of their requests for proposals when pursuing a new system implementation.

As technology evolves, greater integration is needed between the communication and information technology functions. With technologies such as Voice over Internet Protocol (VoIP), a better understanding of the information technology used can shed light on the various security issues that need to be addressed.

Why Does It Matter?

The security of our Nation's emergency response communications infrastructure is an issue that affects us all. Emergency responders must have secure communications to enable them to protect themselves and the lives of citizens. Additionally, the Nation's communications systems must be protected from destructive attacks and intrusions that may lead to wide-ranging disasters. Measures must be taken to ensure the security of these systems so emergency response 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 with changes in 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 emergency response 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 Issues Report—Impediments and Issues on Using Encryption on Public Safety Radio Systems

This report identifies and explains issues and challenges with the development, deployment, and decisions on the use of encryption technologies within the local and state emergency response community. This examination presents factual information and dispels common misinformation about the use of encryption technologies, potential legal ramifications, and operational considerations.

Homeland Security Presidential Directive (HSPD) 7

This directive establishes a national policy for Federal departments and agencies to protect United States critical infrastructure and key resources. For more detailed information on HSPD 7, visit: <http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html>.

To view these and other publications, and for more information on emergency response communications, please visit: <http://www.safecomprogram.gov>.

The SAFECOM program absorbed the Public Safety Wireless Network and its initiatives in 2004. The Office for Interoperability and Compatibility's communications portfolio is currently comprised of the research, development, testing, evaluation, and standards aspects of the SAFECOM and Disaster Management programs.

OFFICE FOR INTEROPERABILITY AND COMPATIBILITY

Defining the Problem

Emergency responders—police officers, fire personnel, emergency medical services—need to share vital voice and data information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies. Unfortunately, for decades, inadequate and unreliable communications have compromised their ability to perform mission-critical duties. Responders often have difficulty communicating when adjacent agencies are assigned to different radio bands, use incompatible proprietary systems and infrastructure, and lack adequate standard operating procedures and effective multi-jurisdictional, multi-disciplinary governance structures.

OIC Background

The Department of Homeland Security (DHS) established the Office for Interoperability and Compatibility (OIC) in 2004 to strengthen and integrate interoperability and compatibility efforts in order to improve local, tribal, state, and Federal emergency response and preparedness. Managed by the Science and Technology Directorate, OIC is assisting in the coordination of interoperability efforts across DHS. OIC programs and initiatives address critical interoperability and compatibility issues. Priority areas include communications, equipment, and training.

OIC Programs

OIC programs address both voice and data interoperability. OIC is creating the capacity for increased levels of interoperability by developing tools, best practices, and methodologies that emergency response agencies can put into effect immediately. OIC is also improving incident response and recovery by developing tools and messaging standards that help emergency responders manage incidents and exchange information in real time.

Practitioner-Driven Approach

OIC is committed to working in partnership with local, tribal, state, and Federal officials in order to serve critical emergency response needs. OIC's programs are unique in that they advocate a "bottom-up" approach. The programs' practitioner-driven governance structures gain from the valuable input of the emergency response community and from local, tribal, state, and Federal policy makers and leaders.

Long-Term Goals

- Strengthen and integrate homeland security activities related to research and development, testing and evaluation, standards, technical assistance, training, and grant funding that pertain to interoperability.
- Provide a single resource for information about and assistance with interoperability and compatibility issues.
- Reduce unnecessary duplication in emergency response programs and unneeded spending on interoperability issues.
- Identify and promote interoperability and compatibility best practices in the emergency response arena.



Homeland
Security