PSWN
Public Safety Wireless Network

Digital Land Mobile Radio (DLMR) Security Problem Statement

Final

June 1998

FOREWORD

This problem statement narrative, presented by the Public Safety Wireless Network (PSWN) program, 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.

Comments regarding the information contained in this document or for more information regarding the purpose and goals of the PSWN please contact the PSWN Program Management Office (PMO) at 800-565-PSWN or see the web page at www.pswn.gov.

Abstract:

National Performance Review (NPR) recommendation IT04, the Public Safety Wireless Network (PSWN) Management Plan, Executive Order 13010, NPR Action Item A06, and the final report from the President's Commission on Critical Infrastructure Protection (PCCIP) have brought to the forefront of national efforts the protection of the evolving public safety communications infrastructure. Evolving public safety digital land mobile radio (DLMR) systems are envisioned as operating as large automated information systems (AIS) with open interfaces providing digital-based interconnectivity with other systems and subsystems. While the latest DLMR technology will increase the efficiency and effectiveness of public safety communications, a host of security risks could be introduced unless effective mitigating actions are undertaken based on security awareness and understanding. Most importantly, digital radio systems must be configured and managed in a way that will provide adequate protection from computer-based threats. Because the majority of DLMR systems now being rolled out across the country are not undergoing any form of security assurance process, the Public Safety Wireless Network (PSWN) program faces the challenge of investigating and addressing the security issues of the public safety communications infrastructure.

The security-related issues facing the PSWN program are the lack of —

- *An understanding of the security threats, vulnerabilities, and risks associated with the evolving DLMR systems;*
- *Clearly specified communications security needs for public safety organizations;*
- *Security standards or guidelines applicable to DLMR systems; and*
- *An understanding of the tools and techniques available to secure these systems.*

This problem statement reflects concerns first raised in the National Performance Review (NPR) Information Technology initiative 04 (IT04) and the Public Safety Wireless Network (PSWN) Management Plan. These concerns have also been reiterated in Executive Order 13010, NPR's "Access America" Action Item A06, and the final report of the President's Commission on Critical Infrastructure Protection (PCCIP), called Critical Foundations, submitted in October 1997. Executive Order 13010, signed on July 15, 1996, calls for the government and private sector to work together to develop a strategy to protect national critical infrastructures from physical, electronic, radio-frequency, and computer-based attacks and to ensure their continued operation. Emergency services, including medical, police, fire, and rescue, were identified as one of the eight critical infrastructures. In addition, A06, which calls for the establishment of an intergovernmental public safety wireless network, includes the requirement to secure all public safety land mobile radio systems. Clearly, the security of public safety communication infrastructures has been identified as an immediate and critical need. The PCCIP report reiterates the need to protect our nation's information and telecommunications infrastructure, including public safety networks.

As with other critical infrastructures, public safety communication systems depend on the latest technologies for optimum operation. Digital land mobile radio (DLMR) systems represent the future of communications for federal, state, and local public safety agencies throughout the United States. This evolution from analog to digital technology and the development of technical standards will result in greater interconnectivity between public safety system components and a broader range of data transferred on public safety networks. An eventual goal, supported by A06 and its predecessor, IT04, is for greater interoperability across what had been communication boundaries between public safety agencies both vertically (between federal, state, and local) and horizontally (within federal, state, or local). This combination of interconnectivity and interoperability among DLMRs will result in large automated information systems (AIS). It is, in large part, the dependence on automated technologies that makes these systems vulnerable to a host of new threats.

Just as the hacker threat poses a serious security risk to improperly protected AISs, that same threat will now apply to the largely computer-controlled digital radio systems. Depending on the specific system's features, DLMR systems may allow computer-based remote reprogramming, rekeying, talkgroup assignment, and the designation of channels for use by specific talkgroups. Careful assignment of privileges to perform these functions is critical for security. Also, if both local and remote access to the consoles that provide these capabilities is not properly controlled, accidental or malicious reconfiguration or disabling of the radio system could occur. Digital radio systems must be configured and managed in a way that will provide adequate protection from computer-based threats.

The increased use of automated technologies is also driving an increase in the transmission of data in public safety communications. For example, the technology now exists for mobile data terminals (MDTs) running specialized applications to query multiple remote databases for a wide variety of information in a short period of time. However, the DLMR architectures that make this type of data transfer possible may also make it more vulnerable. Public safety sensitive but unclassified (SBU) data will then flow on largely unencrypted networks and reside on computers that may be insufficiently protected. Unchecked, the possible entry points into such a network could expand greatly. For example, a single dial-in modem on any computer on a network could expose the network and its data to unauthorized access. As public safety communication systems become more and more interconnected, security vulnerabilities could continue to expand. Just as with voice communications, security services are needed to ensure the integrity, confidentiality, and availability of the system and the data that it transports and stores. Therefore, while the latest DLMR technology will increase the efficiency and effectiveness of public safety communications, a host of security risks could be introduced unless effective mitigating actions are undertaken.

AISs supporting federal operations, including those of the Department of Defense (DoD), are typically subjected to a security-based certification or assurance process during their development life-cycle in accordance with OMB Circular A-130. OMB A-130 states that information should be protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information. State and local governments, conversely, typically lack their own security standards and may look to federal security standards or industry best security practices for guidance in planning, developing, and operating their AISs.

The assurance process is designed to ensure that the necessary technical and procedural security controls are incorporated into the system and its operation to ensure a low level of risk for the overall security of the system. The process may vary between systems, but it typically includes, at a minimum, the development of a security policy, the identification of security requirements, and the performance of a security review (risk assessment) and/or security test and evaluation of the system against its requirements to verify compliance. These requirements may cover a broad range of security domains including computer, personnel, physical, and administrative security. Any failure to meet a requirement may represent a security vulnerability. There is a security risk internal or external to the site if threats exist that could exploit the vulnerability. The majority of DLMR systems now being rolled out across the country are not undergoing any form of security assurance process.

LMR system users and managers may be well aware of traditional LMR security risks and means of protection. Traditional security controls are relatively straightforward and involve the use of some form of encryption for radio frequency (RF) communications, physical protection of equipment, and layers of redundancy in the system for contingency purposes. These individuals, however, are typically unfamiliar with the security threats, vulnerabilities, and resulting risks associated with newer DLMR technologies and system architectures. They may also be unfamiliar with the proper use or configuration of security controls offered with the newer DLMR product lines. The DLMR products may lack appropriate security controls or offer them as optional features. This lack of awareness or understanding of the more AIS-like risks and available security controls associated with modern DLMR systems increases the likelihood that security breaches will occur. Examples of AIS-like technical security controls that may be unfamiliar to traditional LMR users and managers include password protection, file access control, security audit log capture and review, and packet filtering routers or application firewalls to protect interconnected networks. Without appropriate controls, it is more likely that security breaches will go undetected.

The PSWN program, in its overall effort to support the evolution of public safety DLMR systems towards nationwide interoperability, has the challenge of investigating and addressing security issues.

The security-related issues facing the PSWN program are the lack of —

- An understanding of the security threats, vulnerabilities, and risks associated with the evolving DLMR systems;
- Clearly specified communications security needs for public safety organizations;
- Security standards or guidelines applicable to DLMR systems; and
- An understanding of the tools and techniques available to secure these systems.