



*Land Mobile Radio System  
Recommended Security Policy*

**FINAL**

**October 1999**

## **FOREWORD**

This document, presented by the Public Safety Wireless Network (PSWN) program, outlines a recommended security policy for public safety agencies. Public safety agencies may apply this security policy to the design, implementation, and operation of their land mobile radio (LMR) systems. If this policy is implemented and followed, it should improve the overall system security of current and developing public safety LMR systems.

To provide comments on the information in this document or to obtain additional information regarding PSWN's purpose and goals, please contact the PSWN Program Management Office (PMO) at 800-565-PSWN or see the PSWN Web page at [www.pswn.gov](http://www.pswn.gov)

# TABLE OF CONTENTS

Page

<b>1. INTRODUCTION .....</b>	<b>1</b>
1.1 BACKGROUND .....	1
1.2 PURPOSE.....	2
1.3 SCOPE.....	2
1.4 DOCUMENT ORGANIZATION .....	2
<b>2. SECURITY POLICY .....</b>	<b>3</b>
2.1 ADMINISTRATIVE SECURITY .....	3
2.1.1 Security Plans, Procedures, and Documentation .....	3
2.1.2 Contingency Plans.....	4
2.1.3 Security Awareness and Training .....	4
2.1.4 System Development and Maintenance.....	4
2.1.5 Configuration Management.....	5
2.1.6 Software and Data Security.....	5
2.1.7 Personnel Security .....	6
2.2 PHYSICAL SECURITY .....	6
2.3 COMPUTER SECURITY .....	6
2.3.1 Authentication .....	7
2.3.2 Access Control .....	7
2.3.3 Audit .....	7
2.3.4 Object Reuse.....	8
2.4 COMMUNICATIONS SECURITY .....	8
2.4.1 Transmission Security .....	8
2.4.2 Encryption.....	8
2.4.3 Key Management.....	10
2.4.4 Firewall.....	10
2.5 RADIO SECURITY .....	10
2.6 MOBILE DATA TERMINAL/MOBILE COMPUTER TERMINAL SECURITY .....	11
<b>APPENDIX A¾ REFERENCES .....</b>	<b>A-1</b>
<b>APPENDIX B—GLOSSARY.....</b>	<b>B-1</b>
<b>APPENDIX C—ACRONYMS .....</b>	<b>C-1</b>

# 1. INTRODUCTION

Protecting emergency services infrastructure, which includes public safety organizations and their communications systems, presents many challenges for policy makers who influence information technology systems and for the public safety community. Many authorities—Executive Order 13010, National Partnership for Reinventing Government (NPRG) Action Item A06 formerly known as National Performance Review, the final report from the President’s Commission on Critical Infrastructure Protection (PCCIP), and Presidential Decision Directives (PDD) 62 and 63—require that the emergency services infrastructure be protected from physical and cyber threats. The Public Safety Wireless Network (PSWN) Program Management Office (PMO) supports this ongoing requirement by encouraging public safety agencies to prepare for major technology changes that could dramatically affect the security of their communications systems.

This document outlines a recommended security policy that local, state, and federal public safety agencies may use throughout their land mobile radio (LMR) communications systems’ life cycle. Security policy is defined as the set of regulations, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. This security policy can serve as a model for agencies when developing their individual security policies.

## 1.1 Background

Public safety communications systems are evolving from conventional analog LMR systems that process mainly voice communications to interconnected, interoperable, conventional or trunked digital systems that process voice, data, and imagery communications. This evolution has resulted in systems that rely heavily on computer-based technologies, thereby transforming security concerns from those associated with a traditional radio system into those more commonly associated with large, distributed automated information systems (AIS). Initiatives are under way to develop technical standards for the next generation of LMR systems that will be procured by public safety agencies. These developing LMR standards introduce new services and connectivity options that create a substantially more complex communications environment and new avenues for possible threats.

Threats are intentional or unintentional actions taken against a system that can result in the modification, disclosure, or destruction of sensitive or private information or that can degrade or disable system operations. Security vulnerabilities are weaknesses in a system’s protection schemes that may be exploited. The degree of risk associated with a system depends on the likelihood of a threat being carried out and the severity of associated vulnerabilities. Candidates that have been proposed as new LMR standards address security controls to some extent, yet many do not address minimizing the vulnerability of radio systems to computer-based threats.

The *PSWN Digital Land Mobile Radio Risk Assessment Report*, dated January 1998, provides a preliminary security threat and vulnerability assessment of LMR security standards. This assessment emphasizes the generic system model as defined in the Telecommunications

Industry Association/Electronics Industry Association (TIA/EIA) Interim Standards (IS) and Telecommunications Systems Bulletins (TSB) 102 series documents. The risk assessment finds LMR security standards deficient in a number of areas, including authentication, access control, and accountability. These deficiencies result in a host of potential vulnerabilities. The assessment reveals heavy reliance on encryption for confidentiality of communications, rather than the use of AIS-based security features for total system security.

The *PSWN Digital Land Mobile Radio Security Guidelines Recommendations*, dated October 1998, forms the basis for this document and recommends a common set of security guidelines for public safety LMR systems. Establishing security guidelines is considered a critical first step in ensuring the incorporation of adequate security controls and best security practices in public safety LMR systems.

## **1.2 Purpose**

This document provides a recommended security policy for public safety LMR systems. The PSWN program believes that establishing a communications system security policy is a critical first step in ensuring that adequate security controls and best security practices are made a part of the development of new public safety LMR systems.

## **1.3 Scope**

The policy outlined in this document is applicable to planned and operational public safety LMR systems. It addresses areas of administrative security, physical security, computer security, communications security, radio security, and mobile computer terminals (MCT) and mobile data terminals (MDT) as they relate to LMR systems. This security policy has been formulated in accord with a variety of sources, including federal government security policies and industry best security practices.

## **1.4 Document Organization**

The remainder of this document is organized as follows:

- Section 2, Security Policy—Definition of security policies for administrative, physical, computer, communications, radio, and MCT/MDT security
- Appendix A—Reference list of security guidelines sources
- Appendix B—Glossary
- Appendix C—Acronyms.

# 1. SECURITY POLICY

This section defines the recommended radio system security policy in the following areas:

- Administrative security
- Physical security
- Computer security
- Communications security
- Radio security
- MCT/MDT security.

Addressing security in all of these areas is critical because vulnerabilities in any area may negate the effectiveness of security controls in the other areas.

## 2.1 Administrative Security

Administrative security employs established procedural controls to ensure the confidentiality, integrity, and availability of the LMR system. Administrative security is important regardless of the technology employed. Existing analog LMR systems as well as evolving, computer-based LMR systems should have solid administrative security programs. Administrative security policy consists of policy statements about security documentation, security training, system development life-cycle controls, and personnel security.

### 2.1.1 Security Plans, Procedures, and Documentation

A security program must include security plans, procedures, and other documented security safeguards to meet the set of regulations, rules, and practices that direct how an agency manages, protects, and distributes sensitive information and communications. Certain security-related activities should be performed, and security documents should be produced at appropriate points throughout the system development life cycle. The policy for security procedures and documentation is as follows:

1. *A security program, including security plans, procedures, and other documented security safeguards, shall be put in place to meet all rules, regulations, and practices that direct how an agency manages, protects, and distributes sensitive information and communications.*
2. *Security-related activities (e.g., risk assessments and security testing) shall be conducted to ensure that the security plans and procedures are effective. The results of the security activities shall be documented.*

### **2.1.2 Contingency Plans**

The policy requires contingency plans to provide directions for emergency response, backup operations, and post-disaster recovery, should an emergency or disaster occur. The contingency plan policy is as follows:

- 1. Contingency and disaster recovery plans shall be developed that detail continuity of operations and alternative-site arrangements.*
- 2. Contingency plans shall be tested to ensure that they effectively provide the capability to continue service based on system needs and priorities.*
- 3. Contingency plans shall be updated regularly to ensure that they provide continuity of operations for the agency at all times.*
- 4. Adequate alternative paths shall be available to transmit information.*

### **2.1.3 Security Awareness and Training**

Security awareness and training is a continual process that educates all individuals in an agency about its security policy, including best security practices and procedures. Security training can be conducted through scheduled programs or through memorandums and brochures. The security awareness and training policy is as follows:

- 1. Security training shall be provided to all personnel (i.e., agency employees and contractors) who will use or manage the system.*
- 2. Security training shall include radio- and system-related threats and emergency operations.*
- 3. Periodic refresher training shall be provided for each group of users.*
- 4. An ongoing awareness program shall be provided to ensure that all users are kept aware of both old and new threats to the system.*

### **2.1.4 System Development and Maintenance**

The system development and maintenance policy ensures the integrity of the system throughout the system life cycle. Further, the policy ensures that all system software is developed and maintained with the concurrence of authorized personnel. The system development and maintenance policy is as follows:

- 1. System software shall be developed and maintained only with the concurrence of authorized personnel and through the direct access by authorized personnel.*

2. *Software shall be developed in a controlled, secure environment.*
3. *Software developed in a controlled environment shall be delivered to user sites via authorized carriers.*

### **2.1.5 Configuration Management**

The configuration management policy deals with the control of changes made to a system's hardware, software, firmware, documentation, tests, test fixtures, and test documentation throughout the development and operational life of the system. This control is necessary to prevent changes that could negatively affect the security posture of the radio system unless managers are at least aware of potential risks. The configuration management policy is as follows:

1. *Managers shall ensure that proper configuration control begins in the earliest stages of system design and development and that it extends over the full life of the system.*
2. *A configuration management system shall be used to control and document every change made to software and applications.*
3. *All changes made to documentation, hardware, or software shall be reviewed and approved by a designated security official.*
4. *Software version controls shall be implemented.*

### **2.1.6 Software and Data Security**

Radio system managers need to ensure the integrity, confidentiality, and availability of the software that controls their systems' operation and the data the systems process. Therefore, procedural safeguards should be established to protect the software and data from accidental or deliberate modification, destruction, or disclosure. The software and data security policy is as follows:

1. *Object and source code for system software shall be securely stored when not in use by the developer.*
2. *All software development activities shall take place in a controlled facility.*
3. *Source code shall not be delivered to users.*
4. *Sensitive data stored on removable media shall be placed in an appropriately controlled container or facility.*
5. *Critical data shall be backed up regularly and the backup media (e.g., diskettes, tapes) shall be stored in a secure environment.*



### **2.1.7 Personnel Security**

The personnel security policy ensures that all personnel (i.e., agency employees and contractors) with access to the system have the proper need to know for information to which they have access. It also ensures that users with special privileges (e.g., system administrators) are properly investigated before they are given access to the system. The personnel security policy is as follows:

1. *All personnel who have access to the system shall have proper need to know information to which they have access.*
2. *Individuals shall undergo a background investigation before being placed in critical sensitive positions or authorized to bypass significant technical and security controls on the system.*
3. *All routine, on-site maintenance functions shall be performed by hardware and systems software specialists who have been cleared to the highest level of information processed by the system.*

### **2.2 Physical Security**

The physical security policy addresses the protection of communications equipment and facilities that house the equipment. Facilities may include buildings housing communications centers, network management systems, remote tower sites, dispatch centers, and maintenance facilities. This policy addresses facility security and environmental protection. The physical security policy is as follows:

1. *Physical security controls shall be implemented at all sites, including the following:*
  - a) *Access controls for facilities (e.g., electronic access devices, keys, guards)*
  - b) *Proper visual identification of employees and visitors (i.e., badges)*
  - c) *Restriction of access for all unauthorized personnel*
  - d) *Additional access controls for computer and telecommunications rooms*
  - e) *Additional access controls for rooms that house file servers.*
2. *Proper environmental controls (e.g., air conditioning, uninterruptible power supply) shall be provided as appropriate for each facility.*

### **2.3 Computer Security**

A significant feature of evolving LMR systems is the increasing extent to which the radio systems are managed by computerized means. Interfaces between system components are also increasingly likely to occur via network connections.

Computer security is the aspect of security that focuses on computer hardware and software, their use, and networking components. The following subsections describe the four

basic components of computer security (i.e., authentication, access control, audit, and object reuse) and how these relate to LMR systems.

### **2.3.1 Authentication**

The authentication policy ensures that only authorized personnel have access to the system and the information processed by the system. The authentication policy is as follows:

- 1. The proper controls shall be in place to authenticate the identity of users in accord with any access control policies and to validate each user's authorization before allowing the user to access information or services on the system.*
- 2. User account management shall be in place to ensure that only valid users are able to access the information or services on the system.*
- 3. Authentication data shall be protected from unauthorized access.*

### **2.3.2 Access Control**

The access control policy protects LMR information, services, and resources from unauthorized access or tampering. The access control policy is as follows:

- 1. Controls shall be in place to ensure that only personnel with the proper authorization and a need to know are granted access to LMR systems and their resources.*
- 2. Critical system services and resources shall be protected from unauthorized use.*
- 3. Remote access shall be controlled through identification and authentication mechanisms and restricted to a limited number of authorized personnel.*

### **2.3.3 Audit**

The audit policy ensures that all users are held accountable for their actions and that attempted and actual security violations are detected. The audit policy is as follows:

- 1. The system shall create, maintain, and protect an audit trail of security-related events (e.g., log-on, log-off, access to system administrator functions).*
- 2. The security-related events shall be traceable to the user or process responsible for initiating the event.*
- 3. Procedures shall be in place for the regular review of audit data by authorized personnel.*

### **2.3.4 Object Reuse**

The object reuse policy safeguards the confidentiality of information stored in the LMR system and protects it from unauthorized access. The object reuse policy is as follows:

1. *Storage media containing sensitive information shall be completely empty before reassigning that medium to a different user.*

## **2.4 Communications Security**

The communications security policy goal is to ensure the confidentiality and integrity of information transmitted among the LMR system components. Communications security includes transmission security, encryption, key management, and firewall. Policies for each of these areas are provided below. [Refer to the Glossary in Appendix B for definitions of terms used in this section.]

### **2.4.1 Transmission Security**

The transmission security policy is designed to protect transmissions from interception and exploitation by means other than cryptanalysis and from jamming. The transmission policy is as follows:

1. *Controls other than encryption (e.g., frequency-hopping, spread spectrum) shall be in place to provide communications transmissions adequate protection from the threats of interception, exploitation, and both intentional and unintentional interference.*
2. *Controls shall be in place to prevent replay of voice communications.*

### **2.4.2 Encryption**

The purpose of the encryption policy is to protect information being transmitted among communications components or devices by cryptographic means. The encryption policy is as follows:

1. *Cryptographic components shall be used to ensure secure communications over the LMR system.*
2. *End-to-end encryption shall be implemented to ensure secure communications.*
3. *Encryption devices shall be physically secured when unattended or not in use.*
4. *Encryption algorithms shall be as defined for the Federal Information Processing Standards (FIPS) Publication 140-1 Security Requirements for Cryptographic Modules.*
5. *The system shall support over-the-air rekeying of encryption devices.*



### **2.4.3 Key Management**

The key management policy governs procedures for generating, storing, protecting, transferring, loading, using, and destroying cryptographic keying material (i.e., paper tapes, electronic keys, punch cards, and key codes). The key management custodian ensures that all keying material is protected from deliberate or inadvertent disclosure, theft, modification, or destruction. The key management policy is as follows:

- 1. Public keys shall be protected against unauthorized modification and substitution.*
- 2. Procedures shall be in place that ensure proper generation, handling, disposal, and destruction of outdated keying material.*
- 3. Proper management controls shall be in place for trunked keys.*
- 4. Procedures shall be in place to safeguard all cryptographic material.*

### **2.4.4 Firewall**

The main function of a firewall is to centralize access control. The firewall policy governs procedures for protecting an organization's network and its resources from unauthorized access and denial of service. The firewall policy is as follows:

- 1. A firewall shall be configured to deny all services not expressly permitted.*
- 2. A firewall shall provide detailed audit logs of all sessions so that these logs can be reviewed for any anomalies.*
- 3. A firewall shall be physically secured, and server configuration and management shall be performed physically at the server.*
- 4. A firewall shall not support Internet Protocol (IP) routing or forwarding.*
- 5. A firewall shall be configured to rewrite mail address headers to conceal information regarding the internal network.*

### **2.5 Radio Security**

The radio security policy ensures that radio communications will be available to public safety personnel at all times. The radio security policy is as follows:

- 1. Authentication procedures shall be established to ensure the authenticity of radio transmissions.*
- 2. Authentication controls shall be established to ensure that only authorized radios are used for communications.*

3. *Radio systems shall recognize the failure of any repeaters and adjust accordingly to prevent interruption of communications.*
4. *The agency shall have 24-hour, two-way radio capability to provide continuous communications between the officers on duty and the communications center.*
5. *Radio management controls shall be in place throughout the radio life cycle (e.g., inventory control, lost and stolen radio controls, and disposal or destruction of unused radios).*

## **2.6 Mobile Data Terminal/Mobile Computer Terminal Security**

The MDT/MCT security policy ensures that users conducting transactions via MDT/MCTs are properly authenticated and have authorization to use the system. The MDT/MCT security policy is as follows:

1. *Authentication controls and/or procedures shall be set up between the network and MDT/MCTs to prevent unauthorized transactions.*
2. *MDT/MCT management controls shall be in place throughout the terminal life cycle (e.g., inventory control, lost and stolen terminal controls and disposal or destruction of unused terminals)*
3. *Sensitive data shall be cleared from MDT/MCTs before the terminals are released for disposal or destruction.*

## APPENDIX A<sup>3/4</sup> REFERENCES

Commission on Accreditation for Law Enforcement Agencies, *Chapter 81 Communications Standards*, April 1994

Department of Justice, *Federal Bureau of Investigation Automated Data Processing Telecommunications Security Policy*, undated

Department of the Treasury, Directive Publication 71-10, *Security Manual*, April 30, 1993

Digital Land Mobile Radio System Security Guidelines Recommendations, October 1998

Federal Information Processing Standards (FIPS) Publication 112, *Password Usage*, May 30, 1985

Federal Information Processing Standards (FIPS) Publication 140-1, *Security Requirements for Cryptographic Modules*, January 11, 1994

Land Mobile Radio Security Planning Template, July 1999

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Systems*, February 8, 1996

Telecommunications Industry Association/Electronics Industry Association, Interim Standards (TIA/EIA IS), 102.AAAA-A, *Data Encryption Standard (DES) Encryption Protocol*, February 1997

Telecommunications Industry Alliance/Electronics Industry Association, Telecommunications Systems Bulletins (TIA/EIA TSB):

- TIA/EIA TSB 102-A *System and Standards Definition*, November 1995
- TIA/EIA TSB 102.AAAB *Security Services Overview, New Technology Standards Project, Digital Radio Technical Standards*, January 1996
- TIA/EIA TSB 102.AACA *Over-the-Air Rekeying Protocol, New Technologies Standards Project, Digital Radio Technical Standards*, January 1996
- TIA/EIA TSB PN-3594 *Enhanced Digital Access Communications System and Standards Definition*, August 7, 1997

Trans European Trunked Radio (TETRA) System Security Standards 02.22 *Security Objectives and Requirements*, October 18, 1993

## **APPENDIX B—GLOSSARY**

### **Access Control**

A technique used to define or restrict the rights or capabilities of individuals or application programs to communicate with other individuals or application programs or to obtain data from, or place data onto, a storage device.

### **Audit Trail**

A chronological record of system activities that is sufficient to reconstruct and review the sequence of events surrounding or leading up to all transactions and actions performed on or by the system.

### **Authentication**

The process of verifying the identity of a user, terminal, or application program to prevent fraud, abuse, and misuse of services.

### **Automated Information System**

A collection of hardware, software, and firmware configured to collect, communicate, compute, disseminate, or control data.

### **Availability**

The accessibility and usability of service on demand by an authorized entity.

### **Communication Deception**

Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications.

### **Communications Security**

Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security and physical security of COMSEC material.

### **Computer Room**

A facility that houses computer equipment used to store, process, and transmit data (e.g., network servers, workstations, consoles, mainframes, routers).



## **Computer Cryptography**

Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information.

## **Computer Security**

Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware and information being processed, stored, and communicated.

## **Confidentiality**

The protection ensuring that information is not made available or disclosed to unauthorized individuals, entities, or processes.

## **Configuration Management**

The process of controlling modifications to systems, applications, or system documentation. Configuration management protects the system, applications, and documents against unintended and unauthorized modifications.

## **Contingency Plan**

A plan of action to restore the system's critical functions in case normal processing is unavailable for reasons such as natural disasters, equipment failure, or malicious destructive actions.

## **Cryptanalysis**

Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.

## **Cryptography**

Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

## **Cryptographic**

Pertaining to, or concerned with cryptography.

## **Cryptosecurity**

Component of COMSEC resulting from the provision of technically sound cryptosystems and their proper use.

## **Encryption**

The process of transforming plain text into unintelligible form by using a cryptographic system.

## **Firewall**

An electronic boundary that prevents unauthorized users from accessing certain files on a network; or, a computer used to maintain such a boundary.

## **Identification**

A code, user name, card, or token that identifies an individual.

## **Integrity**

The protection that ensures that data has not been altered (modified, inserted, or deleted), repeated, or destroyed in an unauthorized manner, either accidentally or deliberately.

## **Jamming**

The intentional transmission of radio signals that interfere with the reception of signals from another transmitter.

## **Key**

A series of characters used by an encryption algorithm to transform plain text data into encrypted (cipher text) data and vice versa.

## **Key Management**

The process, policies, procedures, and administration encompassing every stage in the life cycle of a cryptographic key, including generation, distribution, entry, use, storage, destruction, and archiving.

## **Land Mobile Radio**

A mobile communications service between land mobile stations or between land mobile stations and base stations.

## **Mobile Computer Terminal**

A computer device located in a vehicle that provides access to remote database files and to communications with the dispatch office.

## **Mobile Data Terminal**

A radio unit installed in a vehicle that provides access to remote database files and to communications with the dispatch office.

## **Over-the-Air Rekeying (OTAR)**

OTAR refers to the distribution of cryptographic keys over the air. A central facility, called a Key Management Facility (KMF), stores all keys used in a system. The KMF distributes keys by first encrypting a key and then transmitting it over the air to subscriber units in the system. Subscribers decrypt the key and store it for use among themselves.

## **Password**

A protected word, phrase, or a string of characters used to authenticate the identity of a user.

## **Public Key**

The key of a public key pair that is published widely.

## **Security Plan**

A document that outlines a site's plan for securing its system.

## **Transmission Security**

The methods used to protect transmission from interception, exploitation, and jamming by means other than encryption.

## **Vulnerability**

A weakness in a system's design or procedure that could be exploited by a threat to gain unauthorized access to a system or degrade the system's availability.

## APPENDIX C—ACRONYMS

AIS	Automated Information System
EIA	Electronics Industry Association
FIPS	Federal Information Processing Standards
IP	Internet Protocol
IS	Interim Standard
KMF	Key Management Facility
LMR	Land Mobile Radio
MCT	Mobile Computer Terminal
MDT	Mobile Data Terminal
NPRG	National Partnership for Reinventing Government
OTAR	Over-the-Air Rekeying
PCCIP	President's Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PMO	Program Management Office
PSWN	Public Safety Wireless Network
TETRA	Trans European Trunked Radio
TIA/EIA	Telecommunication Industry Alliance/Electronics Industry Association
TSB	Telecommunications Systems Bulletins