Public Safety Wireless Network

Land Mobile Radio System Security Planning Template

Final

August 1999

FOREWORD

This document, presented by the Public Safety Wireless Network (PSWN) program, provides a template to guide the development of security plans for public safety wireless systems. Local, state, and federal public safety agencies may apply this template to develop security plans for their land mobile radio (LMR) systems. Security plans provide public safety agencies with the information necessary to minimize security risks associated with their radio systems.

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

TABLE OF CONTENTS

Page

1. INTRODUCTION

Today's rapidly changing technical environment requires public safety agencies to adopt a minimum set of security controls to protect their information technology (IT) resources. Executive Order 13010, National Performance Review Action Item A06, 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. Additionally, PDD 67 requires that critical federal agencies' infrastructures provide continuity of operations in emergency situations. The Public Safety Wireless Network (PSWN) Program Management Office (PMO) is supporting this ongoing requirement by encouraging public safety agencies to prepare for major technology changes that could dramatically affect the security posture of their communications systems.

To ensure secure implementation of a new radio system or secure configuration of an existing radio system, a security plan is necessary as part of the system development life cycle process. This security planning template is intended for use by local, state, and federal public safety agencies in developing security plans for their land mobile radio (LMR) communications systems. The PSWN program recommends that radio managers use this template to develop their security plans and to ensure necessary management support to improve security of their radio systems.

1.1 Purpose

The objective of system security planning is to improve protection of IT resources. All radio communication systems have some level of sensitivity and require protection as part of good system management. It is a good business practice to document the protection of a radio system in a system security plan.

This template provides a guideline for public safety radio system managers to follow when developing their own security plans that document management, technical, and operational controls for radio systems. The security plan shall be viewed as documentation of the structured process for planning adequate, cost-effective security protection of a radio system. The security plan will allow radio managers to accomplish the following objectives:

- Identify the security requirements of the radio system
- Identify the radio system's overall security posture
- Identify the security controls implemented to protect the radio system from its risks and vulnerabilities
- Identify additional security controls that will improve the protection of the radio system resources

- Provide public safety agency management with the information necessary to secure the radio system.

1.2 Scope

This LMR System Security Planning Template follows guidance documented in Office of Management and Budget (OMB) Bulletin 90-18, "Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information," dated July 9, 1990. This template includes brief instructions on how to complete each section and its subsections. Additionally, it provides examples of security controls that may be incorporated into radio systems.

Security plans are living documents that require periodic reviews, modifications, and milestone or completion dates for planned controls. Procedures shall be in place outlining who reviews the plans and follows up on planned controls. In addition, procedures are needed describing how security plans will be used in the authorization process.

This document is a comprehensive template that includes detailed security features to cover any radio applications and systems. This template can readily be tailored to any public safety agency's environment. Additional information may be included in the basic plan, and the structure and the format can be organized according to agency needs as long as the major sections described in this document are adequately covered. The level of detail included within the plan shall be consistent with the criticality and value of the radio system to the organization's mission (i.e., a more detailed plan is required for systems critical to the organization's mission).

1.3 Document Organization

This security planning template is organized as follows:

- Section I provides an introduction to the report, including the purpose, scope, how to use the template, and terminology.
- Section II outlines the system analysis process in terms of system components, functions, and connectivity.
- Section III provides guidance on determining the radio system's sensitivity and the criticality of information transmitted through the radio system components.
- Section IV explains security controls that are to be considered and incorporated into the radio system.
- Section V provides radio managers with an opportunity to include additional comments about the security status of their radio systems.
- Section VI provides an approval or disapproval form for the security plan.

1.4 How To Use The Template

The template is organized and presented as a technical document for use by radio managers responsible for the security of radio systems to enable them to develop their own radio system security plans. When completed, a security plan will document technical information about the system, its security requirements, and the controls implemented to provide protection against potential risks and vulnerabilities. This template provides brief guidance on developing the major sections of a security plan. The heart of the template is Sections 2-4.

Section 2 of the template presents information related to a radio system that defines services that the radio system provides, system components, and system interfaces. Based on the system description, radio managers can identify potential vulnerabilities associated with their systems.

Section 3 of the template provides a list of regulations and directives that provide security policies and procedures for protecting radio systems. To protect sensitive and critical information from unauthorized disclosure, modification or destruction, radio managers must understand the sensitivity and criticality level of the information transmitted among the radio system components. Section 3 provides examples of considerations that radio managers can review to determine the degree of sensitivity and criticality of information and protection needs to mitigate potential vulnerabilities and risks identified in Section 2.

Section 4 of the template provides a comprehensive list of security measures that may mitigate potential vulnerabilities and risks associated with radio systems. Radio managers shall determine security controls that are applicable to their radio systems based on the security level of information and protection needs defined in Section 3. After selecting the status of the security controls, radio managers can determine the overall risk level of their radio systems and actions to be taken to protect the systems (e.g., request of funds to implement additional security controls and secure the configuration of the system).

1.5 Terminology

To ensure a common understanding of the terminology used to explain the security activities and security services, the following definitions are provided for terms used in this report.

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 and/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.

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

Confidentiality. The protection that ensures 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 to system documentation. Configuration management protects the system or applications 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.

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

Identification. A code, user name, cards, 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 maliciously.

Jamming. The intentional transmission of radio signals in order to interfere with the reception of signals from another transmitter.

Key. When used in the context of encryption, a series of characters that are 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 Data Terminal. Radio unit installed in a vehicle that provides access to remote database files and communications with the dispatch office.

Over-the-Air-Rekeying (OTAR). 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 the keys by first encrypting the key and then transmitting it over the air to subscriber units in the system. Subscribers decrypt the keys and store them for use among themselves.

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

Risk. The possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Risk Assessment. The process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

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

Sensitive Information. Information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information.

Threat. An activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.

Vulnerability. A flaw or weakness in a system that may provide an avenue for an intruder, malicious or otherwise, to compromise the security, integrity, or availability of an information system.

Virus. A self-executing program that is hidden from view and that secretly copies itself in such a way as to "infect" parts of the operating system and/or application programs.

2. SYSTEM IDENTIFICATION

Before the plan can be developed, a determination must be made as to which type of plan is required for the system. This section provides basic identifying information about the system: who is responsible for the system, the system functions, and its connectivity.

2.1 System Name and Acronym:

2.2 Responsible Organization: List organization responsible for the overall operation of the system.

2.3 Designated Point of Contact: List individuals to contact for information concerning this security plan and system, security training, security testing, etc.

Name:
Title:
Voice Phone No.:
Fax Phone No.:
E-mail Address:

2.4 System Operator:

___Agency employees Specify: _____
___Contractors Specify: _____

2.5 System Status: ___Operational Date:
___Under Development (Operational Date):
___Under Major Modifications (Operational Date):

2.6 System Description: Briefly describe the site, including location, system configuration, and system component functions.

System location:

Manufacturer:

Coverage (e.g., county, state):

Type of users (e.g., police, fire, emergency medical service):

Number of channels and frequencies:

Number of dispatch centers:

a. System Type

___Analog conventional
___Multicast
___Simulcast
___Analog trunked
___Trunked zone
___Digital conventional
___Digital trunked
___Other (specify):

b. System Application

___ Voice Only
___ Data Only
___ Integrated Voice/Data

c. System Components

___Network management system
___Wireless data system
___Local area network
___Gateway/router
___Modems
___Controller site
___Portable/mobile radios
___Mobile data terminals
___Mobile computer terminals
___Dispatch consoles
___Remote tower sites
___Backup sites

d. System Components Connectivity

___Wireline
___Radio frequency link
___Fiber
___Analog microwave
___Digital microwave

e. Data Connectivity

___Dedicated
___Integrated Services Digital Network (ISDN)
___Public Switched Telecommunications Network (PSTN)

f. Remote Tower Sites

___Site owned
___Site leased
___Collocated with other organization

g. Maintenance Facility

___Owned
___Leased

2.7 System Interconnection/Information Sharing: Provide the following information concerning authorization for connecting to other systems or sharing information.

List of interconnected systems (including Internet):

Name of systems:

Organization owning the other system(s):

Type of interconnection (e.g., Transmission Control Protocol/Internet Protocol [TCP/IP], Dial, Standard Network Architecture [SNA]):

Name and title of authorizing management official(s):

Date of authorization:

Sensitivity level of each system:

Security concerns of the other systems that need to be considered in the protection of this system:

2.8 System Environment: Briefly describe the environment, including any environmental factors that cause special security concerns (e.g., in earthquake zone, high risk of flood or tornado, poor public utilities).

3. SENSITIVITY OF INFORMATION

This section describes the types of information handled by the radio system and thus provides the basis for defining the system's security requirements. The sensitivity and criticality of the information stored within, processed by, or transmitted by the radio system provides a basis for the value of the system and is one of the major factors in risk management. The description will provide information to a variety of users, including:

- Developers who will use it to help design appropriate security controls
- Internal and external auditors evaluating system security measures
- Managers making decisions about the reasonableness of security countermeasures.

The nature of the information sensitivity and criticality must be described in this section. The description must cover applicable regulations, directives, and policies affecting the system and a general description of sensitivity as discussed in the following subsections.

3.1 Applicable Laws or Regulations Affecting the System: List laws and regulations that establish specific requirements for confidentiality, integrity, and availability of the system.

Federal Directives and Regulations

- ☐ Presidential Decision Directive 63 (http://www.fas.org/irp/offdocs/pdd-63.htm)
- ☐ OMB A-130, *Security of Federal Automated Information Resources* (http://www.eff.org/A/Newin/omb.a130.rev2)
- ☐ Executive Order 13010, *Critical Infrastructure Protection* (http://www.info-sec.com/pccip/web/eo13010.html)
- ☐ Computer Security Act of 1987 (http://www.house.gov/science_democrats/archive/compsec1.htm)

Federal Information Processing Standards Publications

- ☐ FIPS PUB 140-1, *Security Requirements for Cryptographic Modules* (http://csrc.ncsl.nist.gov/fips/fips1401.htm)
- ☐ FIPS PUB 46-2, *Data Encryption Standard* (http://www.nist.gov/itl/div897/pubs/fip46-2.htm)

State Regulations

- ☐ State Security Policy and Procedures

Local Regulations

- ☐ Local Security Policy and Procedures

General Guidance

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

- ☐ TIA/EIA TSB 102.AAAB, Project 25, *Security Services Overview, New Technology Standards Project, Digital Radio Technical Standards*

- ☐ TIA/EIA TSB 102.AACA Project 25, *Over-The-Air-Rekeying (OTAR) Protocol, New Technologies Standards Project, Digital Radio Technical Standards*

3.2 Information Sensitivity: Type of sensitive information handled by this system. (Check ALL that apply)

- ☐ Law enforcement
- ☐ Privacy Act information
- ☐ Medical history information
- ☐ Criminal records
- ☐ Other (specify):_____

3.3 General Description of Sensitivity

The purpose of this section is to review the system requirements against the need for availability, integrity, and confidentiality. It is important that the degree of sensitivity of information be assessed by considering the requirements for availability, integrity, and confidentiality of the information. This process shall occur at the beginning of the radio system's life cycle and be reexamined during each life cycle stage.

Through this analysis, the value of the system can be determined. This value is one of the first major factors to be determined in risk management. The security planning process is designed to reduce the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of information stored and processed on the radio system. A risk assessment is a part of an approach to determine adequate, cost-effective security for a system. The risk level of the system is determined based on two factors: 1) the likelihood that vulnerabilities will be exploited, and 2) the impact that the successful exploitation of the vulnerabilities will have on the agency's operation.

A system may need protection for one or more of the following reasons.

A. Confidentiality: The system contains information that requires protection from unauthorized disclosure.

Example of Information Requiring Protection—Confidentiality
Law enforcement information (e.g., criminal records, drug raids), personal information (covered by Privacy Act), medical history information

A. Integrity: The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification, including detection of such activities (e.g., systems critical to safety or life support).

Example of Information Requiring Protection—Integrity
Location of incidents, medical history information

C. Availability: The system contains information or provides services that must be available on a timely basis to meet mission requirements or to avoid substantial losses.

Example of Information Requiring Protection—Availability
Systems critical to safety, life support, hurricane forecasting

3.4 Protection Needs

Describe, in general terms, the information handled by the system and the need for protective measures. Relate the information to each of the three categories (confidentiality, integrity, and availability) shown in the following table and indicate whether the protection requirement is—

- *High*—a critical concern of the system
- *Medium*—an important concern, but not necessarily paramount in the organization's priorities
- *Low*—some minimal level of security is required, but not to the same degree as the preceding categories

System Information Categories	Protection Requirements for Information		
	High	Medium	Low
Confidentiality			
Integrity			
Availability			

Examples of the general statement are provided below.

Examples of a General Protection Requirement Statement

A high degree of security for the system is considered mandatory to protect the confidentiality, integrity, and availability of information. The protection requirements for all system resources are critical concerns for the system.

OR

Confidentiality is not a concern for this system as it contains information intended for immediate release to the general public concerning fires or hurricanes. The integrity of the information, however, is extremely important to ensure that the most accurate information is provided to the public to allow them to make decisions about the safety of their families and property. The most critical concern is to ensure that the system is available at all times to support life-threatening events.

The following tables provide examples to help radio managers determine the level of protection requirements for their radio systems.

Example Confidentiality Considerations	
Evaluation	**Comment**
High	The system transmits public safety information, which if disclosed to unauthorized sources, could result in failure of mission or operations.
Medium	Security requirements for assuring confidentiality are of moderate importance. Having access to the information does not reveal information involving integrity of operations or mission.
Low	The mission of this system is to provide general information to citizens which is made available to the news media forecasters and the general public at all times. None of the information requires protection against disclosure.

Example Integrity Considerations	
Evaluation	**Comment**
High	The system provides communications capabilities among various public safety agencies. Unauthorized or unintentional modification of this information could cause chaos between the agencies, resulting in failure of life support or people safety.
Medium	Assurance of the integrity of the information is required to the extent that destruction of the information would require significant effort to replace. Although corrupted information would present an inconvenience to the agency personnel, most information is backed up regularly.
Low	The system mainly contains messages and reports. Intentional or unintentional modification of the information would not be a major concern for the organization.

Example Availability Considerations	
Evaluation	**Comment**
High	The system contains talk group template programs. Unavailability of the system could result in failure of the organization to meet critical mission requirements (e.g., people safety, life support). The system requires 24-hour access.
Medium	Unavailability of the system could have a limited impact on the organizations mission. Information backups maintained at off-site storage would be sufficient to carry on with the organization's mission to a limited extent.
Low	The system serves primarily as a server for e-mail. Should the system become unavailable, the organization's mission will not be limited.

4. SYSTEM SECURITY CONTROL MEASURES

This section documents the status of security activities and control measures (in-place or planned) that are intended to meet the protection requirements of the system that have been determined in Section 3.

4.1 Status of Security Activities: Please provide dates for the security activities below:

	Date of Last	Date Planned
☐ Design Review	_____	_____
☐ Risk Assessment	_____	_____
☐ Security Reviews	_____	_____
☐ Security Test and Evaluation	_____	_____
☐ Other (Specify):	_____	_____

If there is no risk assessment for the radio system, include a milestone date (month and year) for completion of the risk assessment. If the risk assessment is more than 3 years old, or there have been major changes to the system or functions, include a milestone date (month and year) for completion of a new or updated risk assessment. Assessing the risk to a system shall be an ongoing activity to ensure that new threats and vulnerabilities are identified and appropriate security measures are implemented.

4.2 Weaknesses: Were any security or control weaknesses identified during the last security review of this system?

If "yes," describe the weaknesses.

4.3 Security Control Measures: For each security measure listed, select the appropriate security control measure status in terms of:

In place—Control measures of the type listed are in place and operational, and judged to be effective. Describe in general terms.

Planned—Specific control measures (e.g., new, enhanced) are planned for the radio system. A general description of the planned measures resources involved and expected operational dates shall be provided.

Action Required—Some measures are not planned or implemented, but specific actions are required to protect the system. A general description of the actions, including the resources involved and expected operational dates, shall be provided.

Not Applicable (N/A)—This type of control measure is not needed, cost-effective, or appropriate for the radio system.

A. Management/Administrative Controls: Overall management controls of the radio system. Management controls focus on managing the radio system and its risks. The types of control measures shall be consistent with the need for protection of the radio system. Select appropriate security control measures status and describe the measures in general terms.

1. Assignment of Security Responsibility

1) Security Manager	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Security Officer (for day-to day operations)	☐ In Place	☐ Planned	☐ Action Required	☐N/A

2. Risk Assessment and Management

1) Design stage risk assessment	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Operational risk assessment	☐ In Place	☐ Planned	☐ Action Required	☐N/A
3) Periodic risk assessments	☐ In Place	☐ Planned	☐ Action Required	☐N/A
4) Periodic security reviews	☐ In Place	☐ Planned	☐ Action Required	☐N/A
5) Security testing	☐ In Place	☐ Planned	☐ Action Required	☐N/A

3. Security Documentation

1) Security specifications	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Security Design Documentation	☐ In Place	☐ Planned	☐ Action Required	☐N/A
3) Configuration Management Plan	☐ In Place	☐ Planned	☐ Action Required	☐N/A
4) System Security Plan	☐ In Place	☐ Planned	☐ Action Required	☐N/A
5) Risk Assessment Report	☐ In Place	☐ Planned	☐ Action Required	☐N/A
6) Security Test and Evaluation Report	☐ In Place	☐ Planned	☐ Action Required	☐N/A
7) Memoranda of understanding with interfacing systems	☐ In Place	☐ Planned	☐ Action Required	☐N/A

4. Security Awareness and Training

1) Security training materials	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Emergency operations procedures	☐ In Place	☐ Planned	☐ Action Required	☐N/A
3) Initial security briefing	☐ In Place	☐ Planned	☐ Action Required	☐N/A
4) Refresher training	☐ In Place	☐ Planned	☐ Action Required	☐N/A
5) Exit briefing	☐ In Place	☐ Planned	☐ Action Required	☐N/A

5. Personnel Screening

1) Employee screening before hiring	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Contractor screening	☐ In Place	☐ Planned	☐ Action Required	☐N/A
3) Background investigation based on job level	☐ In Place	☐ Planned	☐ Action Required	☐N/A
4) Maintenance personnel screening	☐ In Place	☐ Planned	☐ Action Required	☐N/A
5) Cleaning personnel screening	☐ In Place	☐ Planned	☐ Action Required	☐N/A

6. Continuity of Support

1) Continuity of Operations Plan (COOP)	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Disaster and Contingency Plans	☐ In Place	☐ Planned	☐ Action Required	☐N/A

3) Backup sites ☐ In Place ☐ Planned ☐ Action Required ☐N/A
4) Alternate sites ☐ In Place ☐ Planned ☐ Action Required ☐N/A
5) Alternate power sources ☐ In Place ☐ Planned ☐ Action Required ☐N/A
6) Alternate path of communications ☐ In Place ☐ Planned ☐ Action Required ☐N/A
7) Regular backup ☐ In Place ☐ Planned ☐ Action Required ☐N/A
8) Off-site storage facility ☐ In Place ☐ Planned ☐ Action Required ☐N/A
9) Emergency operations plans ☐ In Place ☐ Planned ☐ Action Required ☐N/A
10) Regular contingency planning test ☐ In Place ☐ Planned ☐ Action Required ☐N/A

7. Management of Contractors

1) Contractors screening ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Periodic contractors validation reviews ☐ In Place ☐ Planned ☐ Action Required ☐N/A
3) Contractors' system account management ☐ In Place ☐ Planned ☐ Action Required ☐N/A
4) Security training for contractors ☐ In Place ☐ Planned ☐ Action Required ☐N/A

B. Computer/Network Management Controls: Hardware, software, and network controls used to provide automated protection. The types of control measures shall be consistent with the need for protection of the radio system. Select appropriate security control measures status and describe the measures in general terms.

1. User Identification and Authentication

1) Unique user identification (ID) ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) User authentication
   a. Passwords ☐ In Place ☐ Planned ☐ Action Required ☐N/A
   b. Biometrics ☐ In Place ☐ Planned ☐ Action Required ☐N/A
   c. Smart cards ☐ In Place ☐ Planned ☐ Action Required ☐N/A
   d. Token controls ☐ In Place ☐ Planned ☐ Action Required ☐N/A
3) User account management ☐ In Place ☐ Planned ☐ Action Required ☐N/A
4) Disabling inactive user accounts ☐ In Place ☐ Planned ☐ Action Required ☐N/A

2. Access Controls

1) User profiles ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Separation of duties ☐ In Place ☐ Planned ☐ Action Required ☐N/A
3) Privilege assignments ☐ In Place ☐ Planned ☐ Action Required ☐N/A
4) User account lockout ☐ In Place ☐ Planned ☐ Action Required ☐N/A
5) Screen saver ☐ In Place ☐ Planned ☐ Action Required ☐N/A

3. Audit Trails

1) Audit report generation ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Regular audit report reviews ☐ In Place ☐ Planned ☐ Action Required ☐N/A

4. Virus Protection

1) Installation of anti-virus software ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Diskette scanning policy ☐ In Place ☐ Planned ☐ Action Required ☐N/A
3) Regular update of virus software ☐ In Place ☐ Planned ☐ Action Required ☐N/A

5. Dial-in Access

1) User ID	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Passwords	☐ In Place	☐ Planned	☐ Action Required	☐N/A
3) Dial-back mechanism	☐ In Place	☐ Planned	☐ Action Required	☐N/A
4) Strong authentication	☐ In Place	☐ Planned	☐ Action Required	☐N/A
5) User account management	☐ In Place	☐ Planned	☐ Action Required	☐N/A

C. Physical Controls: Controls used to protect the facility, computer center, dispatch center, radio sites, and backup sites. The types of control measures shall be consistent with the need for protection of the radio system. Select appropriate security control measures status and describe the measures in general terms.

1. Facility Protection

1) Fenced perimeters	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Safeguards	☐ In Place	☐ Planned	☐ Action Required	☐N/A
3) Visitor's log	☐ In Place	☐ Planned	☐ Action Required	☐N/A
4) Visitor escort	☐ In Place	☐ Planned	☐ Action Required	☐N/A
5) Electronic access devices	☐ In Place	☐ Planned	☐ Action Required	☐N/A
6) Controlled circuit TV	☐ In Place	☐ Planned	☐ Action Required	☐N/A
7) Alarmed doors	☐ In Place	☐ Planned	☐ Action Required	☐N/A

2. Computer Room(s)

1) Visitor's log	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Visitor escort	☐ In Place	☐ Planned	☐ Action Required	☐N/A
3) Keys	☐ In Place	☐ Planned	☐ Action Required	☐N/A
4) Cipher lock	☐ In Place	☐ Planned	☐ Action Required	☐N/A
5) Electronic access devices	☐ In Place	☐ Planned	☐ Action Required	☐N/A
6) Alarmed doors	☐ In Place	☐ Planned	☐ Action Required	☐N/A

3. Dispatch Center(s)

1) Fenced perimeters	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Safeguards	☐ In Place	☐ Planned	☐ Action Required	☐N/A
3) Visitor's log	☐ In Place	☐ Planned	☐ Action Required	☐N/A
4) Visitor escort	☐ In Place	☐ Planned	☐ Action Required	☐N/A
5) Keys	☐ In Place	☐ Planned	☐ Action Required	☐N/A
6) Cipher lock	☐ In Place	☐ Planned	☐ Action Required	☐N/A
7) Electronic access devices	☐ In Place	☐ Planned	☐ Action Required	☐N/A
8) Controlled circuit TV	☐ In Place	☐ Planned	☐ Action Required	☐N/A
9) Alarmed doors	☐ In Place	☐ Planned	☐ Action Required	☐N/A

4. Remote Tower Sites

1) Fenced perimeters	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Barbed wire	☐ In Place	☐ Planned	☐ Action Required	☐N/A
3) Visitor's log	☐ In Place	☐ Planned	☐ Action Required	☐N/A
4) Visitor escort	☐ In Place	☐ Planned	☐ Action Required	☐N/A
5) Keys	☐ In Place	☐ Planned	☐ Action Required	☐N/A

6) Cipher lock	☐ In Place	☐ Planned	☐ Action Required	☐N/A
7) Electronic access devices	☐ In Place	☐ Planned	☐ Action Required	☐N/A
8) Controlled circuit TV	☐ In Place	☐ Planned	☐ Action Required	☐N/A
9) Alarmed doors	☐ In Place	☐ Planned	☐ Action Required	☐N/A

5. Telecommunications Closet

1) Keys	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Cipher lock	☐ In Place	☐ Planned	☐ Action Required	☐N/A

6. Environmental Protection

1) Fire extinguishers	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Fire suppression systems	☐ In Place	☐ Planned	☐ Action Required	☐N/A
3) Smoke detector	☐ In Place	☐ Planned	☐ Action Required	☐N/A
4) Water sprinkler	☐ In Place	☐ Planned	☐ Action Required	☐N/A
5) Fire alarm system	☐ In Place	☐ Planned	☐ Action Required	☐N/A
6) Lightning protection	☐ In Place	☐ Planned	☐ Action Required	☐N/A
7) Uninterruptible power supply (UPS)	☐ In Place	☐ Planned	☐ Action Required	☐N/A
8) Battery	☐ In Place	☐ Planned	☐ Action Required	☐N/A
9) Generator	☐ In Place	☐ Planned	☐ Action Required	☐N/A
10) Independent air conditioning unit	☐ In Place	☐ Planned	☐ Action Required	☐N/A
11) Raised floor	☐ In Place	☐ Planned	☐ Action Required	☐N/A
12) Emergency lighting	☐ In Place	☐ Planned	☐ Action Required	☐N/A
13) Surge protector	☐ In Place	☐ Planned	☐ Action Required	☐N/A

D. Communications Controls: Controls used to protect information transmitted among radio system components. The types of control measures shall be consistent with the need for protection of the radio system. Select appropriate security control measures status and describe the measures in general terms.

1. Transmission Security

1) Intentional radio channel interference

a. Radio channel interference detection	☐ In Place	☐ Planned	☐ Action Required	☐N/A
b. Automatic interference clearance	☐ In Place	☐ Planned	☐ Action Required	☐N/A

2) Unintentional radio channel interference

a. Radio channel interference detection	☐ In Place	☐ Planned	☐ Action Required	☐N/A
b. Automatic interference clearance	☐ In Place	☐ Planned	☐ Action Required	☐N/A

2. Encryption

1) Voice encryption	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Data encryption	☐ In Place	☐ Planned	☐ Action Required	☐N/A

If encryption is used, explain the type of encryption level and algorithm.

3. Key Management for Encryption

1) Written procedures	☐ In Place	☐ Planned	☐ Action Required	☐N/A
2) Over-the-air-rekeying	☐ In Place	☐ Planned	☐ Action Required	☐N/A
3) Regular key change	☐ In Place	☐ Planned	☐ Action Required	☐N/A

4) Rekey lockout ☐ In Place ☐ Planned ☐ Action Required ☐N/A
5) Key lost key rekey ☐ In Place ☐ Planned ☐ Action Required ☐N/A

4. Trunked Key Management

1) Written procedures ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Access controls for key holders ☐ In Place ☐ Planned ☐ Action Required ☐N/A
3) Regular key reviews ☐ In Place ☐ Planned ☐ Action Required ☐N/A

5. Firewall/Router

1) User ID ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Passwords ☐ In Place ☐ Planned ☐ Action Required ☐N/A
3) Restricted access controls ☐ In Place ☐ Planned ☐ Action Required ☐N/A
4) Audit report generation and regular review ☐ In Place ☐ Planned ☐ Action Required ☐N/A
5) Regular backup ☐ In Place ☐ Planned ☐ Action Required ☐N/A
6) Limited IP Addresses ☐ In Place ☐ Planned ☐ Action Required ☐N/A
7) Packet filtering ☐ In Place ☐ Planned ☐ Action Required ☐N/A
8) Limited network trusted relationships ☐ In Place ☐ Planned ☐ Action Required ☐N/A
9) Network address translation ☐ In Place ☐ Planned ☐ Action Required ☐N/A

E. Radio Controls: Controls used to protect communications using radios. The types of control measures shall be consistent with the need for protection of the radio system. Select appropriate security control measures status and describe the measures in general terms.

1. Radio Authentication

1) Radio user authentication ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Radio unit authentication ☐ In Place ☐ Planned ☐ Action Required ☐N/A
3) Radio user account management ☐ In Place ☐ Planned ☐ Action Required ☐N/A

2. Talk Group Assignment ☐ In Place ☐ Planned ☐ Action Required ☐N/A

1) Restricted access to template files ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Template control reviews ☐ In Place ☐ Planned ☐ Action Required ☐N/A

3. Lost and Stolen Radio Controls

1) Notification procedures ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Over-the-air radio inhibit ☐ In Place ☐ Planned ☐ Action Required ☐N/A
3) Loaned radio controls ☐ In Place ☐ Planned ☐ Action Required ☐N/A

4. Radio Maintenance

1) Inventory controls ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Secure disposal ☐ In Place ☐ Planned ☐ Action Required ☐N/A
3) Secure destruction ☐ In Place ☐ Planned ☐ Action Required ☐N/A
4) Contractor controls ☐ In Place ☐ Planned ☐ Action Required ☐N/A

F. MDTs/MCTs Controls: Controls used to protect communications using MDTs/MCTs. The types of control measures shall be consistent with the need for protection of the radio system. Select appropriate security control measures status and describe the measures in general terms.

1. User Identification and Authentication

1) User ID ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Password ☐ In Place ☐ Planned ☐ Action Required ☐N/A
3) Personal identification number ☐ In Place ☐ Planned ☐ Action Required ☐N/A
4) License tag number ☐ In Place ☐ Planned ☐ Action Required ☐N/A
5) Radio serial number ☐ In Place ☐ Planned ☐ Action Required ☐N/A
6) User account management ☐ In Place ☐ Planned ☐ Action Required ☐N/A

2. Access Controls

1) User account lockout ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Automatic timeout feature ☐ In Place ☐ Planned ☐ Action Required ☐N/A

3. Audit Trails

1) Audit report generation ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Audit report reviews ☐ In Place ☐ Planned ☐ Action Required ☐N/A

4. MDTs/MCTs Maintenance

1) Inventory controls ☐ In Place ☐ Planned ☐ Action Required ☐N/A
2) Secure disposal ☐ In Place ☐ Planned ☐ Action Required ☐N/A
3) Secure destruction ☐ In Place ☐ Planned ☐ Action Required ☐N/A
4) Secure data removal from unused MDTs/MCTs ☐ In Place ☐ Planned ☐ Action Required ☐N/A

5. ADDITIONAL NEEDS AND COMMENTS

This section is intended to provide an opportunity to include additional comments about the security of the subject system and any perceived need for guidance or standards.

6. REVIEW AND APPROVAL SIGNATURES

Plan Development:

Plan Developed by: _____

Responsible Individual: _____

Phone Number: _____

Plan Completion Date: _____

Plan Review:

Review Staff: _____

Telephone Number: _____

☐ APPROVED ☐ DISAPPROVED Date: _____

APPENDIX A¾ REFERENCES

National Institute of Standards and Technology. *Guide for Developing Security Plans for Information Technology Systems*. Special Publication 800-18. December 1998.

Office of Management and Budget. *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*. Bulletin No. 90-08. July 9, 1990.

Office of Management and Budget, Circular A-130. *Management of Federal Information Resources*. Appendix III, "Security of Federal Automated Information Resources." 1996.

Public Law 100-235, Computer Security Act of 1987.

APPENDIX B¾ LIST OF ACRONYMS

COOP	Continuity of Operations Plan
DES	Data Encryption Standard
FIPS PUB	Federal Information Processing Standards Publication
ID	Identification
IS	Interim Standards
ISDN	Integrated Services Digital Network
IT	Information Technology
KMF	Key Management Facility
LMR	Land Mobile Radio
MDT/MCT	Mobile Data Terminal/Mobile Computer Terminal
N/A	Not Applicable
OMB	Office of Management and Budget
OTAR	Over-the-Air Rekeying
PCCIP	President's Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PMO	Program Management Office
PSTN	Public Switched Telecommunications Network
PSWN	Public Safety Wireless Network
SNA	Standard Network Architecture
TCP/IP	Transmission Control Protocol/ Internet Protocol
TD P	Treasury Directive Publication
TIA/EIA	Telecommunications Industry Association/Electronics Industry Association
TSB	Telecommunications Systems Bulletins
UPS	Uninterruptible Power Supply