PUBLIC SAFETY

PSWN PROGRAM

WIRELESS NETWORK

Saving Lives and Property Through Improved Interoperability

Key Management Plan Template for Public Safety Land Mobile Radio Systems

FINAL

February 2002

FOREWORD

This document, presented by the Public Safety Wireless Network (PSWN) program, provides a template to guide the development of key management plans for public safety wireless systems. Local, state, and federal public safety agencies may apply this template to develop key management plans for their land mobile radio (LMR) systems. It is highly recommended that agencies that provide an interoperable capability use this document to establish a foundational set of operational standards for their key management activities. Key management plans provide public safety agencies with the information necessary to handle and safeguard the keying material in support of encryption.

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 at 800-565-PSWN or see the PSWN Web page at www.pswn.gov.

TABLE OF CONTENTS

1. INTRODUCTION 1
   1.1 Purpose 1
   1.2 Scope 2
   1.3 Document Organization 2
   1.4 How to Use the Template 3
2. KEY MANAGEMENT SYSTEM 5
   2.1 Radio System Name and Acronym 5
   2.2 Responsible Organization 5
   2.3 Roles and Responsibilities 5
   2.4 Designated Point of Contact 7
   2.5 Type of Encryption 7
   2.6 Encryption Boundary 7
   2.7 Information Sensitivity 7
   2.8 Key Management System Connectivity 7
3. KEYING SCHEME 8
   3.1 Voice Encryption 8
      3.1.1 Encryption Algorithm 8
      3.1.2 Key Length 8
      3.1.3 Key Lifetime (Cryptoperiod) 8
      3.1.4 Number of Units Holding the Key 9
   3.2 Data Encryption 9
      3.2.1 Encryption Algorithm 9
      3.2.2 Key Length 9
      3.2.3 Key Lifetime (Cryptoperiod) 10
      3.2.4 Number of Units Holding the Key 10
4. KEY MANAGEMENT ARCHITECTURE 11
   4.1 Encryption Key Level 11
   4.2 Key Selection 12
   4.3 Key Management Device 12
   4.4 Key Management Control 12
   4.5 Key Components and Functions 13
5. KEY GENERATION 14
   5.1 Key Generator Type 14
   5.2 Source of Root Key 14
   5.3 Control of Central or Root Keys 14
   5.4 Key Delivery Method 15
6. KEY DISTRIBUTION 16
   6.1 Key Loading Methods 16
   6.2 Location of Key Change 16
   6.3 Over-the-Air Rekeying 16
      6.3.1 OTAR Method 17
      6.3.2 Key Download Method 17
7. KEY STORAGE 18

7.1 Key Storage Method 18
7.2 Key Storage Form 18
7.3 Location of Physical Key Storage 18
7.4 Authentication Methods for Electronic Key Storage 19
7.5 Test Key Storage 19
8. KEY DESTRUCTION 20
8.1 Key Destruction Method 20
8.2 Physical Key Destruction 20
8.3 Emergency Destruction Procedures 20
9. ACCOUNTING 21
9.1 Radio Unit Account 21
9.2 Communications Security Custodian Account 21
9.3 Accounting Reports 21
9.4 Inventory Check 22
10. ACCESS CONTROLS 23
10.1 Technical Controls 23
10.1.1 Authentication Mechanisms 23
10.1.2 Separation of Roles 24
10.1.3 Guidelines for Access Controls 24
10.2 Physical Controls 24
10.2.1 Location of Key Management System Components 24
10.2.2 Access Control Devices 25
10.3 Environmental Controls 25
11. AUDIT 26
11.1 Components Generating Audit Reports 26
11.2 Audit Events 26
11.3 Audit Reviews 26
11.4 Audit Backup 27
12. KEY SYSTEM RECOVERY 28
12.1 System Component Identification 28
12.2 Contingency Events 28
12.3 Continuity of Operations 29
12.4 Immediate Actions To Be Taken 29
12.5 Recovery Procedures 29
13. ADMINISTRATIVE CONTROLS 31
13.1 Security Activities 31
13.2 Security Training 31
13.3 System Maintenance 32
13.3.1 Routine Maintenance 32
13.3.2 Maintenance Personnel 32
13.3.3 Emergency Maintenance 33
14. INCIDENT REPORTING 34
14.1 Security Incidents 34
14.2 Incident Report 34
14.3 Adjudication 36
15. REVIEW AND APPROVAL SIGNATURES 37

APPENDIX A—ACRONYM LIST A-1
APPENDIX B—REFERENCES B-1
APPENDIX C—GLOSSARY C-1

1. INTRODUCTION

Public safety radio communications often contain sensitive and vital information on law enforcement activities. Preserving the private nature of this information is essential to the protection of life and property. Disclosure or modification of this information could severely impact public safety operations and pose a threat to the safety of public safety officials and citizens. Therefore, the public safety community recognizes the need for protected radio transmissions when broadcasting over the air—only encryption can provide this protection.

As public safety agencies recognize the need for encryption, public safety agencies, with or without interoperable functions, must establish consistent key management processes among themselves. The secure distribution, loading, storing, and destroying keys are essential to make encryption implementation effective. Because of the complexity of generating encryption keys and distributing keys to all radio units in a synchronized fashion, there are inherent risks if proper key management processes are not followed during the key life cycle. Compromise of encryption keys could seriously affect the integrity, confidentiality, and availability of sensitive radio communications.

Without proper handling of keys during their life cycle, keys could be compromised, modified, or substituted by unauthorized personnel who could then intercept radio communications, which could result in loss of life and property. Agencies can significantly mitigate this risk by establishing standard key management processes.

The Public Safety Wireless Network (PSWN) Program recommends that agencies establish a key management plan in support of protected land mobile radio (LMR) communications. This key management plan template is intended for public safety agencies to use in developing a plan that will control keys properly throughout their life cycle.

1.1 Purpose

Key management planning ensures the careful and protected generation, distribution, use, storage, and destruction of encryption keys. The objective of key management planning is to improve the protection of keys. This template provides a guideline for public safety radio system managers to follow when developing a key management plan for their radio system with encryption. The plan is intended to provide a structured process for managing encryption keys. With the key management plan, public safety agencies will be able to accomplish the following objectives:

- Identify roles and responsibilities for personnel who generate, use, and maintain keying materials
- Identify the controls implemented to protect keying materials from potential threats
- Identify additional controls that will improve the protection of keying materials

- Provide custodians with the information necessary to perform proper operation and maintenance of key materials.

1.2 Scope

This Key Management Plan Template does not focus on the technical issues of key management processes, but on the administrative and operational management plans. This template includes brief instructions on how to complete each section and its subsections. It also provides security controls that must be considered to protect keys and keying materials.

This template is a living document that can be tailored to any public safety agency's environment while maintaining consistent key management standards. Plan developers can include additional information in the basic plan, and can organize the structure and format according to agency needs as long the resulting agency document adequately covers the major sections described in this template. The level of detail included within the plan must be consistent with the criticality and value of radio transmission to be protected.

1.3 Document Organization

This key management plan template is organized as follows:

- Section 1 introduces this template, including the purpose, scope, and how to use it
- Section 2 defines the key management system for which this plan is written
- Section 3 provides keying scheme
- Section 4 describes the key management system architecture
- Sections 5–8 discuss proper methods for handling keys during their life cycle, including key generation, distribution, storage, and destruction
- Section 9 describes key accountability
- Section 10 describes access controls implemented to protect keys from unauthorized access
- Section 11 describes security audit events and reviews
- Section 12 provides administrative security activities and describes key system recovery in emergency situations
- Section 13 provides an approval form of the plan
- Three appendixes provide supplementary information on a list of acronyms used in the document, references, and glossary.

1.4 How to Use the Template

This template is organized to guide personnel responsible for their agency's key management systems (e.g., communication systems security officer, telecommunications manager) in developing key management plans for their radio systems. When completed, the key management plan will document critical key management controls in place and planned to protect encryption keys and other associated materials during their life cycle, and other controls that should be established and enforced to provide integrity, confidentiality, and availability of keys. This template provides brief guidance on developing major sections of the key management plan. The heart of the template is Sections 2 through 12.

Section 2 describes the key management system with particular attention to the components that use the keys and their environment. This section also describes administrative responsibilities of those whose duties require use of, access to, or who otherwise must be familiar with the requirements for controlling keying materials.

Section 3 provides the keying scheme for voice and data encryption and defines technical parameters associated with the key (e.g., algorithm, key length, key lifetime, and number of subscribers holding the key).

Section 4 provides an overview of the key management system architecture and describes how keys are transferred among the radio system components from the point of generation to the point of communications devices.

Section 5 provides elements that should be considered during the generation of keys whether the keys are generated by the agency or by another agency. If another agency generates the keys, this section should describe proper methods for delivering and receiving keys.

Section 6 defines how keys are loaded ("filled") into radios (e.g., centrally, locally, or remotely), who is responsible for loading new keys into radios, and where the key change is performed. In addition, if the agency has implemented over-the-air-rekeying (OTAR) technology, this section should include a description of the OTAR method for distributing keys to radios.

Section 7 describes the key storage process in electronic media and/or in electronic form. It should describe which storage methods are used after new keys are filled into radios, how many versions can be stored in databases before they are destroyed automatically, and the location of key storage.

Section 8 describes how keys are destroyed when they are no longer required (e.g., manually, automatically, locally, or remotely). It should also describe how test and/or maintenance keys are handled after their lifetime.

Section 9 describes accountability of keys transferred, type of inventories performed, and type of information recorded in accounting records. These accounting records can be useful for investigation of key compromise.

Section 10 defines technical and non-technical controls governing access to physical and electronic keying materials and key management functions in the areas of key generation, distribution, storage, and destruction. Technical controls include proper configuration of security features provided by system components (e.g., user ID and passwords, file permissions and roles, and auditing). Non-technical controls include physical and environmental controls that restrict access to the rooms housing the system components through access control devices and other administrative procedures (e.g., visitor controls).

Section 11 describes audit mechanisms provided by the key management components, how the mechanisms are configured to capture security-related information (e.g., who access the key-related files and directories, changes made to databases), and who is responsible for reviewing and archiving for future use.

Section 12 describes how a key management system can be recovered in case of loss or compromise of system resources. This section should provide detailed procedures to be taken for all personnel, from end users to authorized personnel who investigate any security incidents that have occurred.

2. KEY MANAGEMENT SYSTEM

This section identifies the boundary of the key management system and administrative personnel and their responsibilities assigned to perform key management functions.

2.1 Radio System Name and Acronym

[Provide the name of the radio system that supports encryption and its acronym.]

2.2 Responsible Organization

[Provide the responsible organization within the agency that develops and executes the key management system plan.] It should be noted that rules and regulations should be followed throughout agencies sharing the system to make procedures consistent. Memorandum of Agreement (MOA) should be established between agencies who use the key management system.

2.3 Roles and Responsibilities

[Specify the roles and responsibilities for those who perform key management functions. Each agency may have different roles and responsibilities. Change the sample information provided in the following subsections accordingly.]

Communications System Security Officer/Telecommunications Manager

- Provide security guidance on the implementation of key management
- Establish written guidelines in the form of a key management plan for the handling and safeguarding of keying material
- Ensure that all individuals who handle keying material are fully cognizant of the key management requirements
- Establish and close custodians'/operators' accounts
- Maintain accounting reports
- Verify regularly the inventory of controlled key account
- Establish an audit and inspection program for the verification of the inventory of key management accounts
- Be responsible for receiving and investigating any security-related incidents

- Provide formal training courses for new custodians/operators and regular training thereafter.

Communications Security Custodian[1]

- Perform key management functions on a day-to-day basis
- Protect keying materials and limit access to individuals with a valid need-to-know and clearance, if applicable
- Configure security features of key management system components in accordance with agency policies
- Maintain all required key accounting and related records
- Conduct inventories of all accountable keying material periodically (e.g., semi-annually), upon appointment or termination of a custodian or as required by the organization
- Perform routine destruction of key material
- Maintain up-to-date records and submit all required accounting reports
- Ensure that all material received is inspected for evidence of tampering
- Report immediately any known or suspected incident involving keying material and submit incident reports.

Radio Technicians/Field Technicians

- Be responsible for filling new keys into radios
- Protect key variable loaders (KVL) before/after filling new keys into radios
- Maintain logs containing information on radio IDs and date/time to fill new keys.

End Users (Subscribers)

- Protect radios with encryption keys in all situations
- Bring radios to the designated locations for new keys to be filled
- Ensure that keys are zerorized in emergency situations, if feasible
- Notify proper personnel of lost or compromised keys.

This section should also address procedures for handling temporary absence of the custodian, change of custodian, and permanent departure of the custodian.

---

[1] *Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules and NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government.*

2.4 Designated Point of Contact

[List the individual(s) responsible for managing the key management plan and who serves as the communications security custodian(s) and operator(s).]

Name:
Title:
Office Address:
Telephone Number:
Fax Number:
E-Mail Address:

2.5 Type of System

☐ Voice ☐ Data ☐ Voice/Data

2.6 Encryption Boundary

[Specify the boundary of encryption.]

☐ Within the agency
☐ Inter-agency

2.7 Information Sensitivity

[Specify the type of information protected through encryption. (Check all that apply.)]

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

2.8 Key Management System Connectivity

[Specify the connectivity of the key management system to any other systems within the agency or outside the agency]

☐ Stand-alone system
☐ Private network (closed network)
☐ Open network within the organization
☐ Internet

3. KEYING SCHEME

This section defines technical parameters associated with each key to be used (e.g., algorithm, key length, key lifetime, etc.)

3.1 Voice Encryption

3.1.1 Encryption Algorithm

[Indicate the type of algorithm used and specifications compliant.]

☐ Data Encryption Standard (DES)
☐ Triple DES (TDES)
☐ Advanced Encryption Standard (AES)
☐ Proprietary encryption algorithm

Key Specification Compliant

☐ FIPS PUB 46-3, Data Encryption Standard
☐ FIPS PUB 140-2, Security Requirements for Cryptographic Modules
☐ FIPS PUB 197, Advanced Encryption Standard
☐ TIA/EIA 102 Standard

3.l.2 Key Length

[Indicate the key length.]

☐ 64 bits
☐ 112 bits
☐ 128 bits
☐ 196 bits
☐ 256 bits

3.1.3 Key Lifetime (Cryptoperiod)

[Indicate frequency of key change.]

☐ Monthly
☐ Semi-annually
☐ Annually
☐ Other (Specify):

3.1.4 Number of Units Holding the Key

[Indicate the number of subscribers using the key.]

Subscribers	Portable Radios	Mobile Radios	Key Variable Loaders	Digital Interface Units	Key Management Facility
Within the agency					
Outside the agency					
TOTAL					

3.2 Data Encryption

3.2.1 Encryption Algorithm

[Indicate the type of algorithm used and specifications compliant.]

☐ Data Encryption Standard (DES)
☐ Triple DES (3DES)
☐ Advanced Encryption Standard (AES)
☐ Proprietary encryption algorithm

Key Specification Compliant

☐ FIPS PUB 46-3, Data Encryption Standard
☐ FIPS PUB 140-2, Security Requirements for Cryptographic Modules
☐ FIPS PUB 197, Advanced Encryption Standard
☐ TIA/EIA 102 Standard

3.2.2 Key Length

[Indicate the key length.]

☐ 64 bits
☐ 112 bits
☐ 128 bits
☐ 196 bits
☐ 256 bits

3.2.3 Key Lifetime (Cryptoperiod)

[Indicate frequency of key change.]

- ☐ Monthly
- ☐ Semi-annually
- ☐ Annually
- ☐ Other (specify):

3.2.4 Number of Units Holding the Key

[Indicate the number of subscribers using the key.]

Subscribers	Portable Radios	Mobile Radios	Key Variable Loaders	Digital Interface Units	Key Management Facility
Within the agency					
Outside the agency					
TOTAL					

4. KEY MANAGEMENT ARCHITECTURE

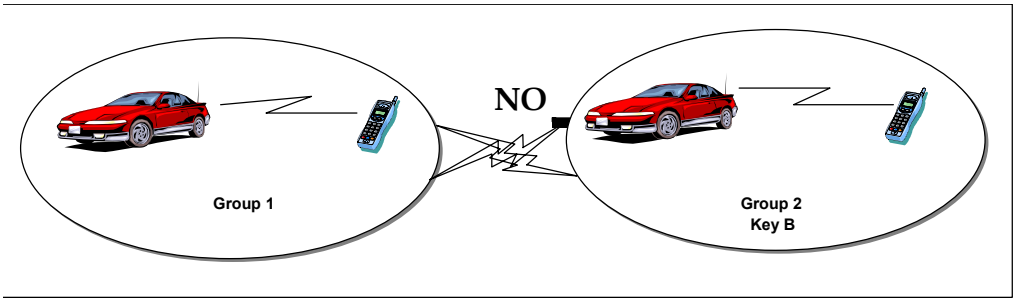
This section provides an overview of the key management system configuration. If the agency uses the OTAR method, this section should also describe any key related OTAR structure.

4.1 Encryption Key Level

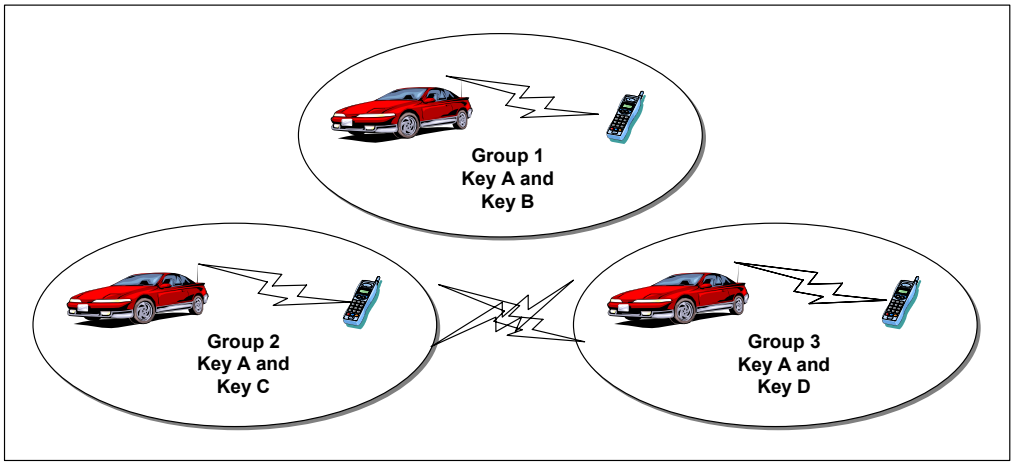
[Select the key levels that the system supports and provide detailed information on how keys are assigned to different groups. Also, if the system supports multi-keys, indicate the number of keys radios can have. System level security is equal to the highest level of key used in the system. Provide diagrams presenting key levels. (See sample diagrams below.)]

- ☐ Single key (subscribers' radios capable of one encryption key per radio)
- ☐ Multi-keys (communications between groups with different keys)
- ☐ Group partitioning
- ☐ Interoperability (pre-planned mapping of keys) – To avoid constant changes, preplanned mapping is critical.

Example Diagram of Single Key



Example Diagram of Interoperability



4.2 Key Selection

[If interoperability is provided, describe how keys are selected for interoperability.]

- ☐ Channel slaved (e.g., user selects slaved channel key; it is set during programming, which requires minimal user interface)

- ☐ User selectable (e.g., two-step, menu-driven process; user selects channel and key separately; provides increased flexibility).

4.3 Key Management Device

[Specify the computer devices used for key management functions, number of the devices and their locations, and functions of each device. If more than one device is used, describe the relationship between the devices.]

- ☐ Key Management Facility (KMF) (used with digital LMR network and uses standards-based signaling for key encryption)

- ☐ Key Management Controller (KMC) (used with analog LMR network and uses proprietary data signaling for key encryption)

- ☐ KMF and KMC

- ☐ Manual Key Fill, Key Variable Loader

4.4 Key Management Control

[Specify the status of key management centers and describe how the key management controls are performed in a hierarchical structure or distributed environment.]

- ☐ Centralized control of key management (master control center)
- ☐ Multiple key management centers
- ☐ Manual and automated

Central control over all key management functions ensures uniform implementation of key management, which promotes cost-effectiveness and interoperability, and assures uniform end-user security training for implementing key management requirements.

4.5 Key Components and Functions

[Indicate all components used to perform key management functions and provide their functions.]

Components	Functions
☐ KMF server	Acts as the main server for the key management functions on the network
☐ KMF client workstation	Provides operator interface to the OTAR and key management functions
☐ Wireless Network Gateway	Manages message routing between the data/KMF network and the radio frequency network
☐ Radio Network Controller	Routes data messages and managed message traffic over the radio system.
☐ Key Variable Loader	Used for loading keys into radios or other network devices.
☐ Ethernet Hub/Switch	Provides Ethernet connectivity to all devices on KMF data network.
☐ Other (specify):	

5. KEY GENERATION

The generation of keys is the most sensitive of all key management functions. This section should describe any security measures in place and planned to protect all automated resources that generate root keys and initialization vectors (IV) from unauthorized disclosure, insertion, and deletion of the keys produced by the system. It is essential to maintain the security of the central or roots keys from the generation process. If these keys are compromised, a complete system compromise becomes a real threat.

5.1 Key Generation Method

[Describe how the key is generated.]

- ☐ Random Number Generator
- ☐ Pseudorandom Number Generator
- ☐ Manual Generation
- ☐ Automatic Generation

5.2 Source of Root Key

[Indicate sources that generate root keys. Encryption keys may or may not be generated by public safety agencies.]

- ☐ Public safety agency
- ☐ National Security Agency (NSA)
- ☐ Other (specify):

5.3 Key Types

[Indicate different keys that the KMC/KMF supports.]

Traffic Key

- ☐ Interoperability key
- ☐ Agency-specific key
- ☐ Test key

Key Encryption Key

- ☐ Interoperability key
- ☐ Agency-specific key
- ☐ Test key

5.4 Control of Central or Root Keys

[Describe how the generation of central or root keys is controlled.]

- ☐ Split knowledge
- ☐ Dual control
- ☐ Other (specify):

5.5 Key Delivery Method

[If a key is not generated by the agency, describe reasons for receiving keys from other agencies, how the keys are delivered to the organization from the point of generation, and detailed controls involved in the key delivery and receipt process.]

- ☐ Courier
- ☐ Regular mail
- ☐ Sealed package
- ☐ Secure voice
- ☐ Receipt of key
- ☐ Other (specify):

6. KEY DISTRIBUTION

After a key is generated, it should be loaded ("filled") into radios. Different techniques are used to distribute encryption keys, depending on radio systems' capabilities. The following subsections provide key load methods and frequency of key distribution. This section should provide detailed information on the key distribution methods and techniques.

6.1 Key Loading Methods

[Indicate which key filling methods are used and describe the methods in detail. (Note: The first encryption key is filled into radios manually.)]

- ☐ Manual
- ☐ Automatic (Over-the-air rekeying [OTAR])
- ☐ Manual and automatic
- ☐ Individual radios
- ☐ Groups of radios

6.2 Location of Key Change

[If keys are manually changed, indicate where keys are changed and controls in place and planned to protect radios being brought in.]

- ☐ Field sites (Radio technicians go out into the field.)
- ☐ Central location (Radio users bring their radios to the location.)
- ☐ Other (specify):

6.3 Over-the-Air Rekeying

[If the OTAR technique is used, describe how OTAR is performed, any components used to perform OTAR, and protection controls involved in OTAR.]

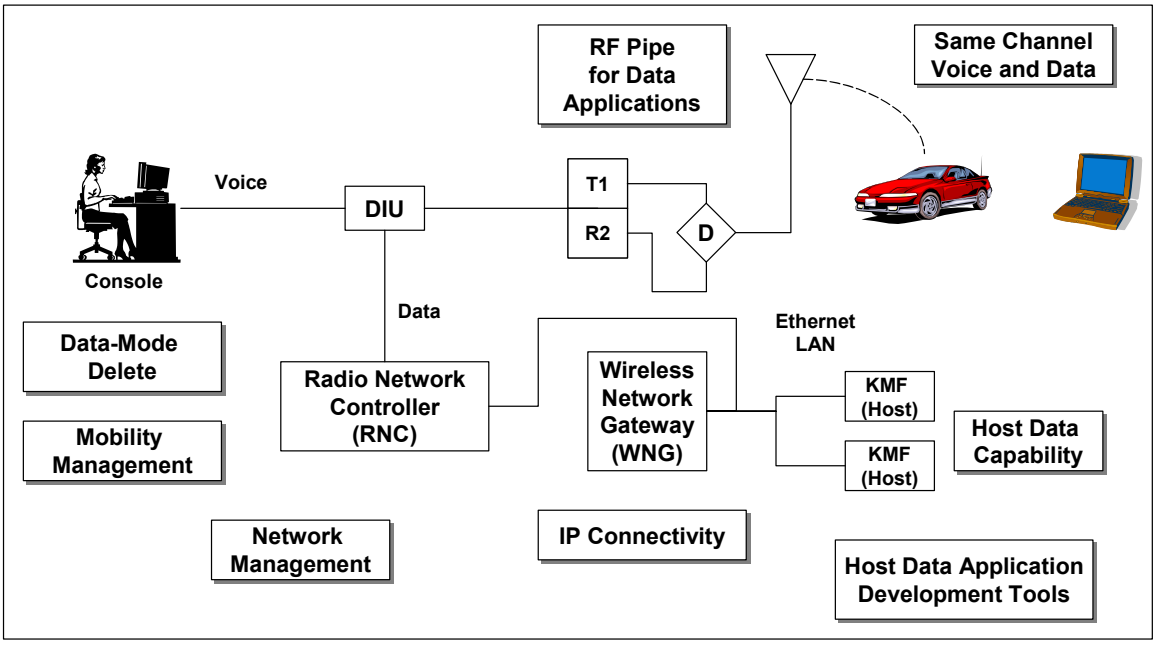
OTAR allows subscriber radios or base equipment to receive new keys or other rekeying information from a KMF over the RF channel or a wireline connection. OTAR increases security, efficiency, and productivity by allowing more rekeys, allowing rekeying many radios in seconds, and providing centralized key management. OTAR uses the data mode of the Common Air Interface (CAI) to exchange OTAR messages between a KMF and radios to support the encryption of voice and data. The OTAR protocol complies with TIA 102 facility key management.

6.3.1 OTAR Method

[Select one of the key flows and describe how keys flow from the point of generation to subscribers. Provide a diagram. (See sample diagram below.)]

- ☐ Proprietary OTAR
- ☐ TIA 102 OTAR (Conventional)
- ☐ TIA 102 OTAR (Trunked)

TIA 102 OTAR Method



6.3.2 Key Download Method

[Describe methods used to fill new keys into KVLs when OTAR cannot be used because the radio(s) is out of range.]

- ☐ Direct cable connection
- ☐ Telephone circuit
- ☐ Modems to a remote KVL

7. KEY STORAGE

Once keys are generated, they must be stored properly to prevent unauthorized persons from accessing, using, or compromising them. The session keys and the key encrypting keys must be kept in protected storage. If keys or key components are generally stored on a token (e.g., diskettes or tapes), this token may need to be stored in a special manner to prevent unauthorized individuals from accessing the key or key components. Additionally, keys should be stored in encrypted format on electronic media. The original keys can also be stored in the computer until they are deleted automatically.

7.1 Key Storage Method

[Describe where the active and inactive keys are stored after they are generated and after they are filled into radios.]

Active Keys

- ☐ Physical key in removable electronic media (describe the type of media)
- ☐ Electronic form in the key database
- ☐ Both storage methods
- ☐ Other (specify):

Inactive Keys

- ☐ Physical key in removable electronic media (describe the type of media)
- ☐ Electronic form in the key database
- ☐ Both storage methods
- ☐ Other (specify):

7.2 Key Storage Form

[Describe how keys are stored in the KMF and in the electronic media. If a key is stored in encrypted form, describe how it is encrypted (e.g., session keys are encrypted).]

- ☐ Clear form
- ☐ Encrypted form

7.3 Location of Physical Key Storage

[If keys are stored in removable media, indicated where the media are stored, the location of the stored devices, and the controls for protecting the storage devices.]

- ☐ Locked drawer
- ☐ Vault
- ☐ Protected computer room

- ☐ Separate office from the computer room
- ☐ Other (specify):

7.4 Authentication Methods for Electronic Key Storage

[If keys are stored in an electronic format, describe detailed controls in place and planned to prevent unauthorized disclosure and ensure key integrity.]

- ☐ User identification
- ☐ Passwords
- ☐ Personal Information Number
- ☐ Smartcard
- ☐ Other (specify):

7.5 Test Key Storage

[Describe how the test key is used and stored. The test key may be used as a maintenance key.]

- ☐ Destroy the test key after the system or device becomes operational
- ☐ Use the test key as a maintenance key

8. KEY DESTRUCTION

Key destruction involves a variety of mechanisms, including zeroizing of keys in a cryptomodule, or removal disabling of a key in the user key database. In addition, this section should describe methods for destroying encryption keys filled into radios.

8.1 Key Destruction Method

[Describe method for destroying keys in electronic form or in physical form.]

- ☐ Automatic destruction (e.g., the number of old versions to be retained [e.g., five old versions])
- ☐ Manual destruction (e.g., physical media destruction)
- ☐ Over-the-air zeroization
- ☐ Manual key zeroization

8.2 Physical Key Destruction

[Describe how encryption keys stored in media are destroyed after use.]

- ☐ Purge
- ☐ Overwrite
- ☐ Destruction of media (e.g., burning, shredding, pulping)

8.3 Emergency Destruction Procedures

[Describe how encryption keys stored in radios are destroyed in emergency situations.]

- ☐ Over-the-air zeroization
- ☐ Manual key zeroization

9. ACCOUNTING

This section describes how radios filled with keys are individually accounted for and how accountability is transferred when keys are transferred. It also describes what types of inventories are performed and types of information contained in accounting reports.

9.1 Radio Unit Account

[Describe detailed procedures for assigning a number to an individual radio.]

- ☐ Accountable by serial number
- ☐ Accountable by radio unit ID
- ☐ Call sign
- ☐ Individual account
- ☐ Group account

9.2 Communications Security Custodian Account

[Describe procedures for creating and deleting custodian accounts and who is responsible for maintaining user accounts.]

Describe the following procedures:

- Requesting a custodian account (e.g., submit a formal form with responsibilities)
- Establishing the account (e.g., role-based, identity-based authentication)
- Closing the account (e.g., when the account is no longer required).

9.3 Accounting Reports

[Accounting reports are prepared to record the transfer, possession, inventory, and destruction of keying materials. Describe type of information recorded in the accounting reports, who maintains the accounting reports; when the reports are reviewed, and detailed procedures for submitting the reports.]

Type of software generating accounting reports [Describe how to avoid assigning duplicate radio unit IDs.]

- ☐ *Database*
- ☐ *Spreadsheet*
- ☐ *Word Processor*

Type of Accounting Reports

- ☐ Transfer Report—Used to record keying material transferred from one point to another point
- ☐ Destruction Report—Used to report the physical destruction of keying material

☐ Inventory Report—Used to report the physical inventory of keying material
☐ Possession Report—Used to report the possession of keying material that is not included on a Transfer Report

Information contained in accounting reports
☐ Official titles
☐ Account number
☐ Date/time of report
☐ Actions involved (e.g., transfer, receipt, destruction)
☐ Persons responsible for identified actions
☐ Other (specify):

Frequency of generating accounting reports
☐ Monthly
☐ Semi-annually
☐ Whenever custodians are changed.
☐ Other (specify):

9.4 Inventory Check

[Describe how the agency performs an inventory.]

A physical inventory of all accountable keying material will be conducted regularly (e.g., semi-annually) by the custodian and alternate custodian. Any material no longer required must be identified and re-marked properly. The custodian will perform special inventories if loss or compromise of keying material is suspected.

Frequency of Inventory Check
☐ Monthly
☐ Semi-annually
☐ Annually
☐ Other (specify):

Type of Information contained in the Inventory List
☐ Equipment ID (e.g., KVL, radio unit ID)
☐ Serial Number
☐ Person performing inventory
☐ Date/time of inventory
☐ Equipment owner
☐ Other (specify):

10. ACCESS CONTROLS

This section describes technical and non-technical (physical) access controls governing access to physical and electronic keying materials and key management functions (e.g., generation, distribution, storage, and destruction). If the agency uses a computer-controlled machine to generate, store, and delete encryption keys, this section should provide a detailed description of operating system and software running on the machine and controls provided by the components.

10.1 Technical Controls

The following table is a sample list of key management components and controls provided to prevent unauthorized access. The actual description of control methods and constraints should be more detailed. These controls should be compliance with the agency's regulations.

Key Management System Components Controls				
Device/ Application	**OS/Platform**	**User ID/ Password**	**Access Controls**	**Audit**
KMF server	Windows NT	User ID/ password	Permissions for files and directories are configured properly.	OS only
KMF client	Windows NT	User ID/ password	Access to the client workstation is restricted to a limited number of people.	OS & Application
Wireless Network Gateway	IBM AIX	User ID/ password	Permissions for files and directories are configured properly.	OS only
Radio Network Controller	Embedded OS	None		N
Key Variable Loader	Embedded OS	Personal Identification Number (PIN)		Y
Ethernet Hub/Switch	Embedded OS	N/A		N/A

10.1.1 Authentication Mechanisms

[Select type of authentication mechanisms used and describe detailed constraints provided.]

☐ Password
☐ PIN
☐ Smart Card
☐ Other (specify):

Password Constraints [If passwords are used, specify password constraints in place and planned.]

☐ Minimum password length (eight alpha-numeric combination)

- ☐ Password age (30 days)
- ☐ Password history (five password uniqueness)
- ☐ Account lockout feature after three invalid login attempts
- ☐ Authentication time-out feature

10.1.2 Separation of Roles

[Describe how the custodian's privileges are assigned.]

- ☐ Separation of roles (different roles handle separate functions)
- ☐ No separation of roles

10.1.3 Guidelines for Access Controls

[Specify the guidelines used to configure security features of the system components.]

- ☐ Vendor-provided Windows NT Security Checklists
- ☐ NSA Windows NT Security Configuration Guidelines
- ☐ Vendor-provided Unix Security Checklists
- ☐ NSA UNIX Security Configuration Guidelines
- ☐ Other (specify):

10.2 Physical Controls

Any inadequacies in the physical security safeguards will seriously undermine the security of the cryptographic mechanisms. It is imperative that the physical security measures are in place to protect the key management facility. In addition, rooms must be provided to restrict access to both the key management system and the keys generated therein to prevent unauthorized disclosure, insertion, and deletion of the system files and keys produced by the system.

10.2.1 Location of Key Management System Components

[Identify the location where the encryption components reside, including KMF/KMC servers and clients.]

- ☐ Computer/network room
- ☐ Isolated Office
- ☐ Office with other system equipment
- ☐ Other (specify):

10.2.2 Access Control Devices

[Identify physical access mechanisms for the facility/room where the system components reside to prevent unauthorized access.]

- ☐ Electronic access device
- ☐ Cipher combination locks
- ☐ Key
- ☐ Visitor controls (e.g., logs, badges, and escorts)
- ☐ Locked all the time
- ☐ Locked whenever nobody is present
- ☐ Security alarms
- ☐ Sensor systems
- ☐ Video systems

Describe how the room is staffed.

- ☐ Supervision for 24 hours a day/7 days a week
- ☐ During the working hours

10.3 Environmental Controls

[Describe environmental controls in place and planned to protect key management system equipment from disastrous situations (e.g., water, fire, failure of air conditioning.]

Type of environmental controls

- ☐ Fire extinguishers
- ☐ Individual air conditioning
- ☐ Humidity controls
- ☐ Emergency lighting
- ☐ Uninterruptible power supply

Frequency of equipment test

- ☐ Semi-annually
- ☐ Annually

11. AUDIT

This section describes auditing and logging functions associated with the key management system.

11.1 Components Generating Audit Reports

[Indicate which system components provide a capability of generating audit logs and which ones are configured to capture security-related information.]

- ☐ KMF server
- ☐ KMF client
- ☐ Wireless Network Gateway
- ☐ Network Controller

11.2 Audit Events

[If audit logs are generated, indicate which events are logged in the audit reports for each component.]

KMF Server

- ☐ Start-up and shutdown of the system
- ☐ Any attempt to modify or delete key-related files and directories
- ☐ Successful and failed logins and logoffs
- ☐ Addition or deletion of custodian role
- ☐ Attempts to provide invalid input for custodian functions
- ☐ Other (specify):

11.3 Audit Reviews

[Indicate who is designated to review audit reports and how often the reports are reviewed.]

Personnel responsible for reviewing audit reports

- ☐ Telecommunications Manager
- ☐ Communications System Security Officer

Frequency of reviewing audit reports

☐ Daily ☐ Weekly ☐ Other

11.4 Audit Backup

[Describe how often audit reports are backed up and where the backup tapes are stored.]

Frequency of Audit Backup

☐ Incremental daily backup
☐ Full weekly backup
☐ Other (specify):

Storage of Audit Backup

☐ Computer room
☐ Tape room
☐ Off-site
☐ Other (specify):

12. KEY SYSTEM RECOVERY

This section describes the process of recovering critical keys stored in the key management system if the key management system or keys are compromised or destroyed intentionally or unintentionally due to various threats (e.g., hardware failure, human threats, environmental or natural disasters). Each agency should prepare a plan to describe detailed actions to be taken by personnel responsible for operating and managing the key management system.

This plan should provide workable procedures and information to minimize the functional impact of threats that may be potentially disruptive to continued key management functions. This section should not be used as system's contingency plans. Detailed contingency plans for the key management system must be developed and followed.

12.1 System Component Identification

[List an inventory of all critical and essential key management components.]

- ☐ Key management system hardware and software
- ☐ Key variable loaders
- ☐ Key accounts
- ☐ Other key equipment

12.2 Contingency Events

[Define contingency events that could cause loss of keys.]

- ☐ Keys received in a damaged package
- ☐ Key management application programming errors
- ☐ Unauthorized modification or destruction of keys
- ☐ Key loss during OTAR transmission
- ☐ Lost or stolen radios with encryption keys
- ☐ Interception of radio transmissions
- ☐ Tampering with encryption equipment
- ☐ Environmental threats (e.g., fire, sabotage, bomb explosion)
- ☐ Natural disasters (e.g., winter storm, lightning, tornado, hurricane, earthquake)
- ☐ Other (Specify):

12.3 Continuity of Operations

[Depending on the contingency event, minimum operations of key management can be provided based on the prepared actions before the event occurs.]

- ☐ Key Personnel Notification Roster – identify those who will be the immediate contacts for key loss or destruction and recovery
- ☐ Fault Tolerance and Redundancy – The key management system should have the capability to provide a unnoticeable interruption of operations with equipment features in place to support redundant or backup storage of keying materials
- ☐ Spare Equipment – provide spare system components (e.g., KMF servers, radios)
- ☐ Backup media – Back up system resources regularly and store backup media in a protected environment
- ☐ Periodic Testing – Test the key management contingency plans regularly
- ☐ Service Agreement – Establish a service level agreement with vendors for emergency services and supplies.

12.4 Immediate Actions To Be Taken

The following are example actions to be taken in an effort to restore compromised keys. To assess the impact, these questions should be answered:

- Is the key recoverable?
- If the key is recoverable, what state is the key in?
- If the key was involved in a compromising situation, to what extent could this key be exposed? To what extent was the keying material compromised? Can integrity be maintained?
- If the key was damaged, to what extent is the damage?
- What can be done now to suppress the incident?

12.5 Recovery Procedures

After assessing the event and the state of the key, appropriate recovery procedures can go in effect. When keys are compromised or damaged, the following procedures should be considered:

If the key stored in the KMF/KMC is destroyed,

- ☐ Retrieve backup media containing active keys
- ☐ Examine whether the key stored in the media is the latest version
- ☐ Upload the key into the KMF/KMC

If keys are compromised,

- ☐ Destroy the compromised key in a proper manner
- ☐ Inform radio users of the situation
- ☐ Generate a new key
- ☐ Follow the normal procedures for generating, distributing, and storing keys

13. ADMINISTRATIVE CONTROLS

This section describes administrative and management controls to ensure key management functions are performed properly during their life cycle and the system is protected from potential threats.

13.1 Security Activities

[Indicate any security activities performed and to be performed related to encryption key management activities.]

- ☐ Develop key management policy and requirements (in the areas of functional, assurance, and environmental)
- ☐ Perform vulnerability/risk assessments (to identify threats and vulnerabilities associated with the key management system)
- ☐ Develop user and crypto-custodian guides

13.2 Security Training

[Describe how security training is provided to personnel responsible for handling, managing, and using encryption keys and keying materials.]

All personnel who handle or have access to keying materials must ensure that their performance is compliant with the agency's control procedures and that they are familiar with security procedures for performing proper key management functions through regular security training sessions or manuals.

Frequency of Security Training

- ☐ Initially (before custodians are granted access to the key management system)
- ☐ Regularly (annually, semi-annually)

Immediately after the submission of a request for the appointment of a Custodian, that individual must attend the Custodian Training Course. Custodians must attend refresher courses and regular training courses thereafter.

Security Training Materials

- ☐ User guide manual
- ☐ Brochure
- ☐ Video/tapes
- ☐ Formal training sessions

Topics included in the Training

- ☐ Roles and responsibilities
- ☐ Threats and vulnerabilities associated with a key management system

- ☐ Installation of cryptographic software and hardware
- ☐ Loading and execution of cryptographic processes
- ☐ Security functions and features provided by encryption devices
- ☐ Computer-controlled security features in the areas of user ID and passwords, privilege assignment, and auditing
- ☐ Physical security controls
- ☐ Incident report procedures

13.3 System Maintenance

Maintenance of key management system components is critical to ensure the secure operation and availability of the module. The following maintenance areas must be considered.

13.3.1 Routine Maintenance

[Provide procedures for regular maintenance to ensure availability of the system.]

- ☐ Hardware/firmware
- ☐ Software maintenance/update (e.g., operating systems, key database, network software)

Maintenance Period

- ☐ Once a year
- ☐ Every 6 months
- ☐ Other (specify):

Location of Maintenance

- ☐ On site (maintenance logs)
- ☐ Through modem (If a modem is used, describe detailed controls in place, e.g., dial-back, manual connection, user ID and password)
- ☐ Other (specify):

13.3.2 Maintenance Personnel

[Indicate who performs encryption components maintenance and provide detailed controls in place and planned to protect the components and keys stored in the components]

- ☐ Organization personnel
- ☐ Vendor/contractor

If vendor/contractor performs the maintenance, indicate controls in place.

- ☐ Background investigation
- ☐ Maintenance activities monitoring
- ☐ Maintenance logs

13.3.3 Emergency Maintenance

[Indicate who performs emergency maintenance and procedures.]

- ☐ Organization personnel
- ☐ Vendor/contractor

14. INCIDENT REPORTING

This section describes procedures for reporting security-related incidents.

14.1 Security Incidents

Every person who uses, handles, or otherwise accesses key material must report security incidents immediately to authorized personnel (e.g., Supervisor, Security Officer). Incidents could include—

- Unauthorized use of key for other than its intended purpose
- Unauthorized extension of a crypto period
- Premature use of key
- Maintenance of keying material by unqualified personnel
- Tampering with keying material or system
- Theft of keying material
- Unauthorized disclosure of key information
- Keying material left unsecured and unattended where unauthorized persons could have had access
- Keying material received in a damaged package
- Failure to zerorize within the required time.

14.2 Incident Report

The report should include the following information:

- Material involved
- Personnel involved
- Location of incident
- Circumstances of incident
- Additional reporting requirements which will include specific incidents or items
- Possibility of compromise
- Point of contact.

The following table illustrates a sample incident report.

Encryption Key Security Incident Report		
Agency Name: [County, State or Regional Law Enforcement Agency name]	Key Account Number/Radio Unit Account Number (if applicable):	
Keying Material Involved: [Keys, equipment, radio, computer system, etc.]	Personnel Involved: [Those responsible for the incident]	
Incident Description: [Chronological account of events as they transpired. Include relevant dates, frequency of events, times of day, locations and agency elements involved. Also include any security measures that went into effect.]		
Additional Details: [Based on incident. If any of the following occurred, please list the required details: Improper Use of Keys: Communications mode, operational mode of the equipment, amount and type of traffic involved, length of time key was used. Malfunctioning Equipment: Symptoms, possible cause (intentional or unintentional), amount and type of traffic involved. Corruption, Sabotage: Individual's knowledge of encryption key management, system access Key Loss: Last sighting of material, actions taken to locate the material, possibility of unauthorized access. Keys discovered outside of protected environment: corrective physical measures, length of time unsecured, likelihood of unauthorized access. Keys Received in a Damaged or Tampered Package: Evidence of damage or tampering, estimate of when the damage occurred along transit route, estimate of the likelihood of unauthorized access or viewing. Unauthorized access to equipment or material: Description of suspected modification, time the material was accessed]		
Initial Corrective Action Taken:		
Current State of Key: [Compromised/Damaged/Lost/Destroyed]		
Personnel Reporting Event:	Personnel Developing Report:	Point of Contact:

14.3 Adjudication

After the initial incident report, a decision based on the background of the incident should occur, which will resolve any misconduct and rectify any incorrect procedures. The Communications System Security Officer, after review of the report, shall submit a recommendation for resolution based on four means of action. There are several options relating to both the keys involved and the incident: Key Recovery, Key Destruction, Disciplinary Action, and Resolution. All options are explained below.

- Key System Recovery

  Section 12 of this document describes the procedures for recovering keys.

- Key Destruction

  If the key involved was compromised or damaged, it will be necessary to immediately destroy or recover enough of the key to gain access to other material and schedule the key for destruction at a later time.

- Investigation and Implementing Disciplinary Action

  Investigative efforts shall gather enough background information on the incident to substantiate an appropriate decision. These efforts are at the agency's discretion. For example, if it is determined that the violation is not valid, the report and other documentation shall be destroyed. If the violation is valid, written notification of the action shall be provided to the individual responsible for the violation. The security official or the bureau concerned shall recommend to the respective management official or bureau head that disciplinary action be taken.

- Resolution

  After the decision is made, a final report of the incident should be written detailing the final corrective actions taken to resolve the incident, as well as recommended preventive measures.

15. 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 A—ACRONYM LIST

The following acronym list applies to the current template. When developing the agency plan, modify this list to reflect the actual plan.

AES	Advanced Encryption Standard
CAI	Common Air Interface
DES	Data Encryption Standard
DIU	Digital Interface Unit
IP	Internet Protocol
IV	Initialization Vector
KMC	Key Management Controller
KMF	Key Management Facility
KVL	Key Variable Loader
LMR	Land Mobile Radio
NSA	National Security Agency
OTAR	Over-the-Air Rekeying
PIN	Personal Identification Number
PSWN	Public Safety Wireless Network
RF	Radio Frequency
TDES	Triple Data Encryption Standard

APPENDIX B—REFERENCES

Federal Information Processing Standard 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001.

Federal Information Processing Standard 171, *Key Management Using ANSI X9.17*, April 27, 1992.

Federal Information Processing Standard 46-3, *Data Encryption Standard*, October 25, 1999.

Federal Information Processing Standard 197, *Advanced Encryption Standard,* November 26, 2001.

National Security Agency Manual 90-2, *COMSEC Material Control Manual*, October 1989.

NIST Special Publication 800-21, *Guideline for Implementing Cryptography in the Federal Government*, November 1999.

Public Safety Wireless Network Program, *Introduction to Encryption for Public Safety Radio Systems*, October 2001.

APPENDIX C—GLOSSARY

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.

Algorithm. A set of mathematical rules (logic) used in the processes of encryption and decryption.

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.

Automated Key Distribution. The distribution of cryptographic keys, usually in encrypted form, using electronic means such as a computer network.

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.

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

Encryption Key. A parameter used in conjunction with a cryptographic algorithm that determines the transformation of plaintext data into ciphertext data or the transformation of ciphertext data into plaintext data.

Cryptoperiod. The time span during which a specific key is authorized for use or in which the keys for a given system may remain in effect.

Decryption. The process of changing ciphertext into plaintext.

Dual Control. A process of using two or more separate entities (usually persons) operating in concert, to protect sensitive functions or information.

Encryption. The process of transforming plaintext into unintelligible form by using a cryptographic system.

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

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

Interoperability. The condition achieved among communications-electronics systems or equipment when information can be exchanged directly between them and their users.

Key. A series of characters used by an encryption algorithm to transform plaintext 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.

Key Management Controller. An electronic device (desktop computer) used with analog LMR network and uses proprietary data signaling for key encryption.

Key Management Facility. An electronic device (desktop computer) used with digital LMR network and uses standards based signaling for key encryption.

Key Variable Loader. A hand-held device used to load encryption keys into a radio.

Keying Material. Key, code, or authentication information in physical or magnetic form.

Key Encrypting Key. A cryptographic key used for the encryption or decryption of other keys.

Maintenance Key. Key intended only for off-the-air, in shop, use.

Over-the-Air Rekeying. OTAR refers to the distribution of cryptographic keys by transmitting the information over a radio system.

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

Remote Rekeying. Secure electrical distribution of a key by radio or wire/fiber optical line.

Server. Computer device or process that provides service to clients in a client/server architecture.

Session Key. The secret (symmetric) key used to encrypt each set of data on a transaction basis. A different session key or set of session keys is used for each communication session.

Split Knowledge. A condition under which two or more entities separately have key components that individually convey knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module.

Telecommunications Manager. The person designated in writing by proper authority to be responsible for the generating, storing, safeguarding, and destruction of keying materials.
Test Key. Key intended for "on-the-air" testing of key equipment.

Threat(s). Person, thing, event, or idea that poses some danger to an asset. The occurrence of a threat might compromise the confidentiality, integrity, or availability of an asset by exploiting vulnerabilities.

Zeroization: A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.