Public Safety Wireless Network

Digital Land Mobile Radio (DLMR) System Security Guidelines Recommendations

Final

October 1998

FOREWORD

This document, presented by the Public Safety Wireless Network (PSWN) program, identifies recommended system security guidelines, including industry best security practices. Local, state, and federal public safety agencies may apply these system security guidelines to the design, implementation, and operation of their digital land mobile radio (DLMR) systems. Implementation of these guidelines, if followed, should improve overall system security among current and developing public safety DLMR systems.

To provide comments regarding the information contained 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

Protecting the emergency services infrastructure, which includes public safety and the communication system they use, is a challenge now faced by the public safety community. 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 62/63) require that the emergency services infrastructure be protected from physical and cyber threats. 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 communication systems. This document presents recommended security guidelines which local, state, and federal public safety agencies may draw upon during their digital land mobile radio (DLMR) communication systems' life cycles. These security guidelines may also be used to develop the agencies' security policies.

1.1 Background

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

Security threats are intentional or unintentional actions taken against a system that could result in the modification, disclosure, or destruction of sensitive or privacy information or that could impact or disable system operations. Security vulnerabilities are weaknesses in a system's protection schemes that may be exploited by threats. The degree of risk associated with a system is dependent on the likelihood of threats occurring and the severity of associated vulnerabilities. Emerging candidates for DLMR standards address security controls to some extent, yet many do not address minimizing vulnerabilities of radio systems to computer-based threats.

The *PSWN DLMR Risk Assessment Report (For Official Use Only)*, dated January 1998, provides a preliminary security threat and vulnerability assessment of DLMR security standards. Specific emphasis was placed on the generic system model as defined in the Telecommunications Industry Association/Electronics Industry Association (TIA/EIA) Interim Standards (IS) and Telecommunications Systems Bulletins (TSB) 102 series documents. This risk assessment found DLMR security standards lacking in a number of areas, including authentication, access control, and accountability, resulting in a host of potential vulnerabilities. The assessment revealed heavy

reliance on encryption for confidentiality of communications rather than the use of AIS-based security features for total system security.

1.2 Purpose

This document recommends a common set of security guidelines for public safety DLMR systems. Establishing security guidelines is thought to be a critical first step in ensuring the incorporation of adequate security controls and best security practices within public safety DLMR systems.

Figure 1 illustrates the intended use of the guidelines identified in this document. In using these guidelines, each agency must determine the applicability of each guideline to its system based on factors such as sensitivity of information transferred, criticality of operations, and requirements to interoperate with other systems that require strong security controls. Beyond providing guidance to public safety agencies, these guidelines have additional value. The guidelines could be used to evaluate the security protection offered by existing DLMR system components or technologies to a DLMR system. Comparisons of component security features across vendors, using evaluation criteria derived from these guidelines, would provide public safety agencies with valuable information to aid in their system procurement and integration process. In addition, systems' compliance with the appropriate guidelines could be used as the basis for risk assessments performed for planned or operational DLMR systems.

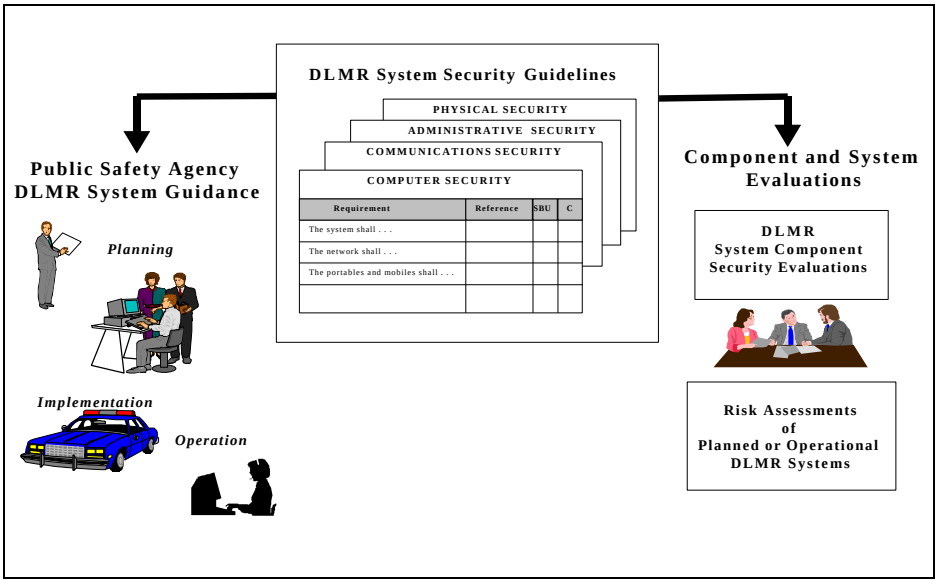

Figure 1
Primary Purposes of DLMR Security Guidelines

1.3 Scope

The guidelines contained in this document are applicable to planned and operational public safety DLMR systems. They address areas of administrative security, physical security, computer security (COMPUSEC), communications security (COMSEC) as they relate to DLMR systems. These security guidelines have been extracted or derived from a variety of sources including Federal Government security requirements and industry best security practices.

1.4 Document Organization

This document is organized as follows:

- Section 1, Introduction—provides background, purpose, scope, and document layout
- Section 2, Security Guidelines Identification Approach—describes steps taken to identify security guidelines
- Section 3, Security Guidelines Organization—describes processes used to organize security guidelines
- Appendix A—Reference List of Security Guidelines Sources
- Appendix B—Administrative Security Guidelines
- Appendix C—Physical Security Guidelines
- Appendix D—Computer Security (COMPUSEC) Guidelines
- Appendix E—Communications Security (COMSEC) Guidelines

2.

GUIDELINES IDENTIFICATION APPROACH

This section describes the approach taken to identify, document, and organize guidelines for public safety DLMR systems. Figure 2 illustrates this approach, which consists of four steps.

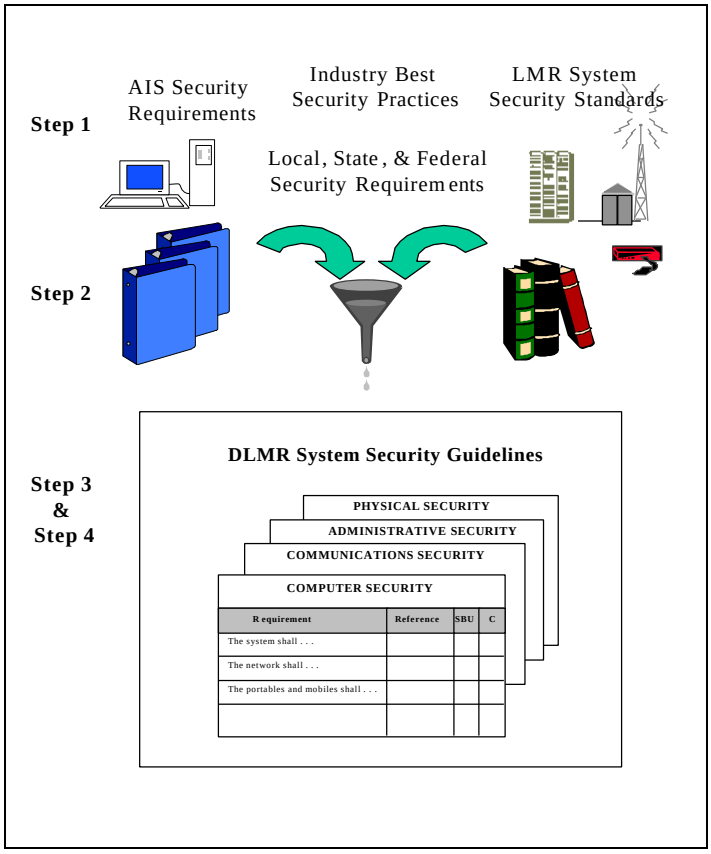

Figure 2
Security Guidelines Development Process

Step 1: Gather and Review Resource Information

The first step in identifing DLMR security guidelines was to gather and review existing local, state, and federal DLMR and AIS security requirements, guidelines, and standards, as well as industry best security practices. Appendix A lists these sources by their full titles and their abbreviated titles for future reference.

Step 2: Identify and Document Applicable Security Guidelines

Security guidelines applicable to DLMR systems were identified and extracted from the various sources identified in Step 1.

Step 3: Organize Applicable Guidelines by Category

The identified guidelines were organized into the following four major security areas: 1) administrative security, 2) physical security, 3) computer security, and 4) communications security. These major areas were then further subdivided into more specific categories. Finally, system components to which each guideline may apply were identified. The resulting guideline organization is described in Section 3.

Step 4: Identify and Map Security Guidelines to Sensitivity Levels

Two data security levels, sensitive but unclassified (SBU) and classified (C), were defined, and each guideline was examined to determine the level to which it applied. The guidelines were then mapped to one or both security levels by annotating the appropriate columns in the guideline tables. Representing security guidelines in this manner should provide agencies with additional guidance when incorporating security mechanisms into their systems. The final guideline tables are provided in Appendixes B through E.

3.

SECURITY GUIDELINES ORGANIZATION

This section describes the organization of security guidelines and defines the categories to which they have been assigned. The guidelines were categorized into the following four major security areas:

- Administrative Security
- Physical Security
- COMPUSEC
- COMSEC

Addressing security in all of these areas is critical because vulnerabilities in any one of the areas may negate the effectiveness of security controls in the other areas. three of these four security areas were further divided into subcategories. The rationale for the selection of the four broad categories and for the subcategories is described in the following subsections.

3.1 Administrative Security

Administrative security is the employment of established procedural controls to ensure the confidentiality, integrity, and availability of the DLMR system. Although DLMR systems may be evolving toward more automation and dependence on technical or computer-based controls, those controls alone are not sufficient, making administrative security vital. For example, computers that support radio system management may offer strong authentication controls. However, those controls may be obviated unless strict policies are followed that address such issues as user account management and other highly privileged capabilities.

3.1.1 Security Plans, Procedures, and Documentation

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

3.1.2 Contingency Plans

Contingency plans are documented plans that provide directions for emergency response, backup operations, and post-disaster recovery. These plans should be maintained by an agency as a part of its security program to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation (e.g., natural disaster or system failure). Radio systems must be designed to provide continuous communications in the event of hardware malfunction or in degraded states, ensuring reliability and availability through technical features and architectural redundancy.

3.1.3 Security Awareness and Training

Security awareness and training is a continual process whereby all individuals of an agency are educated regarding the agency's security policy, including best security practices and procedures, either formally through scheduled programs or informally through scheduled events.

3.1.4 Configuration Management

Configuration management is the control of changes made to a system's hardware, software, firmware, documentation, tests, test fixtures, and test documentation throughout the development and operational life of the system. This control is necessary to ensure that changes are not made that could negatively affect the security posture of the radio system without managers at least being aware of potential risks.

3.1.5 Software & Data Security

Radio system managers need to assure the integrity, confidentiality, and availability of the software that controls their systems' operation and the data that they process. Therefore, procedural safeguards should be established to protect the software and data from accidental or malicious modification, destruction, or disclosure.

3.1.6 Personnel Security

Security procedures should be established to ensure that all agency personnel who have access to any sensitive information have the required authorizations and all appropriate clearances. In addition, personnel who are responsible for managing critical systems should have the need-to-know to carry out privileged duties.

3.2 Physical Security

Managers of radio system sites should address physical security through the implementation of appropriate physical barriers and procedural controls as preventative measures or countermeasures against threats to resources and sensitive information. Physical controls address the protection of all facilities where system components are housed, including remote tower sites and maintenance facilities. Physical security controls should also address the security of the equipment itself, both in its operational environment and while being transported for maintenance purposes.

3.3 Computer Security

A significant feature of evolving DLMR systems is the greater extent to which the radio systems are managed through computerized means. There is also the likelihood of an increased number of interfaces between system components via network connections. Although these changes greatly increase the flexibility and manageability of the systems, they also may introduce

additional computer security risks if these new capabilities are not configured and managed securely. To effectively address these security issues, guidelines traditionally considered when evaluating AISs should be adopted for DLMR systems.

COMPUSEC is that aspect of security that focuses on computer hardware and software, its use, and networking components. The following subsections describe the four basic components of COMPUSEC and how they apply to DLMR systems. Because of the variety of DLMR system components that may be computer based, the guidelines are further identified as being applicable to system components or groups of components.

3.3.1 Authentication

Authentication is the act of verifying the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to system resources. The authentication guidelines reflect the assumption that public safety DLMR system managers will use a userID/password mechanism for computer-based user authentication control as opposed to more sophisticated and costly means such as token-based authentication (e.g., SecureID) or biometrics (e.g., voice recognition, retinal scans).

3.3.2 Access Control

Access control is the process of limiting access to the resources of a system to only authorized users, programs, processes, or other systems in a network. Various personnel may be responsible for managing different aspects of a radio system. Although the assignments of specific privileges to specific users are often based on job function, the means of enforcing the separation of privileges is managed by technical controls that limit or grant access based on user identity or role.

3.3.3 Audit

The ability to audit the actions of a user of a system, along with the use of individually assigned authentication controls, provides for accountability. Audit records provide security managers with a means to detect misuse or intrusion and identify sensitive data exposed, and possibly track the source of the security breach.

3.3.4 Object Reuse

Object reuse is the concept of clearing a storage medium of any residual data (e.g., files and directories) before reassigning that medium to a different user. As addressed in the object reuse guidelines, any privacy or sensitive information that is no longer needed should be completely deleted to ensure that the information cannot be recovered by any means.

3.4 Communications Security

Communications security guidelines are aimed at ensuring the confidentiality and integrity of radio communications in a DLMR system. Communications security includes transmission security, encryption, and the associated key management.

3.4.1 Transmission Security

Transmission security consists of all measures designed to protect transmissions from interception and exploitation by means other than cryptoanalysis and from jamming. These measures may include such practices as frequency hopping and spread spectrum.

3.4.2 Encryption

Encryption is used to protect information transmitted among communications components/devices by cryptographic means. Secure communications are achieved in a radio system by using cryptographic components embedded in the radios and keys. Only those radios having appropriate cryptographic keys may communicate with one another. Cryptographic components may use various cryptographic algorithms.

3.4.3 Key Management

Key management is the process by which a key is generated, stored, protected, transferred, loaded, used, and destroyed. Devices such as radios can be either manually (physically) or electronically keyed via over-the-air-rekeying (OTAR) techniques in which encryption key is changed in remote crypto-equipment by sending new key directly to the remote crypto-equipment over the communication path it secures. Key management must be performed in such a way that keys are protected from deliberate or inadvertent disclosure, modification, or destruction.

3.5 Security Guidelines Category Summary Table

Table 1 presents a summary of the security guidelines organization. Included is a sampling of specific topics that each guideline subcategory covers.

Table 1
Security Guidelines Categorization

SECURITY CATEGORIES			
ADMINISTRATIVE	**PHYSICAL**	**COMPUTER**	**COMMUNICATIONS**
• Security Plans, Procedures, & Documentation • Configuration Management • Software and Data Security • Contingency Planning • Security Awareness and Training • Personnel Security	• Facility Access and Environmental Controls	• Authentication – Source ID – Receiver ID – User Account – Password • Access Control – Access Privileges – Resource Controls – Component Controls • Audit – Audit Generation – Audit Events – Audit Review • Object Reuse	• Transmission Security – Transmission protection • Encryption – Encryption Services – Encryption Algorithms • Key Management – Key Generation – Key Distribution – Key Maintenance

APPENDIX A¾ REFERENCES

1. References Included

Following are those references that were reviewed and included in the list of security guideline references.

- Department of Justice, *Federal Bureau of Investigation (FBI) Automated Data Processing Telecommunications (ADPT) Security Policy*.
- Department of Treasury Directive Pamphlet (TD P) 71-10, *Security Manual*, April 30, 1993.
- Department of Treasury Directive (TD) 85-02, *Automated Information Systems, Security and Risk Management Program*, April 24, 1987.
- Federal Information Processing Standards Publications (FIPS PUB) 112, *Password Usage*, May 30, 1985.
- Federal Information Processing Standards Publications (FIPS PUB) 140-1, *Security Requirements for Cryptographic Modules*, January 11, 1994.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Systems*, February 8, 1996.
- Commission on Accreditation for Law Enforcement Agencies (CALEA), *Chapter 81 Communications Standards*, April 1994.
- Telecommunications Industry Association/Electronics Industry Association, Interim Standards (TIA/EIA IS), 102.AAAA-A, *Data Encryption Standard (DES) Encryption Protocol*, February 1997.
- Telecommunications Industry Association/Electronics Industry Association, Telecommunications Systems Bulletins (TIA/EIA TSB):
  - TIA/EIA TSB 102-A, APCO Project 25, *System and Standards Definition*, November 1995.
  - TIA/EIA TSB 102.AAAB, APCO Project 25, *Security Services Overview, New Technology Standards Project, Digital Radio Technical Standards*, January 1996.

  - TIA/EIA TSB 102.AACA, APCO Project 25, *Over-The-Air-Rekeying (OTAR) Protocol, New Technologies Standards Project, Digital Radio Technical Standards*, January 1996.

  - TIA/EIA TSB PN-3594, *Enhanced Digital Access Communications System (EDACS) System and Standards Definition*, August 7, 1997.

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

2. References Reviewed but Not Included

Following are those references reviewed, but not included in the list of security guideline references because they contain the same security requirements addressed in other Federal Government directives and policies or they do not contain any specific security requirements relevant to DLMR communications.

- Federal Information Processing Standards Publications (FIPS PUB) 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, May 30, 1975.

- Federal Information Processing Standards Publications (FIPS PUB) 73, *Guidelines for Security of Computer Applications*, June 30, 1980.

- Federal Information Processing Standards Publications (FIPS PUB) 83, *Guidelines on User Authentication Techniques for Computer Network Access Control*, September 29, 1980.

- Federal Information Processing Standards Publications (FIPS PUB) 191, *Guidelines for the Analysis of Local Area Network Security*, November 9, 1994.

- National Association of State Telecommunications Directors (NASTD), *State Telecommunications Survey Report*, 1997.

- Title 47 of the Code of Federal Regulations (47CFR), *Telecommunications*, October 1, 1997.

APPENDIX B—ADMINISTRATIVE SECURITY GUIDELINES

DLMR Security Recommendations ADMINISTRATIVE SECURITY				
Requirement		**Reference**	**SBU**	**C**
SECURITY PLANS, PROCEDURES, AND DOCUMENTATION				
AD-1	A system security program shall be implemented and maintained.	OMB A-130, III, A.3	•	•
AD-2	A set of rules of behavior shall be established concerning use of, security in, and the acceptable level of risk for, the system.	OMB A-130, III, 3.a.2.a		•
AD-3	A management official knowledgeable in information technology and security matters shall be assigned for security of the major system.	OMB A-130, III, 3.a.1	•	•
AD-4	Sensitive information shall be protected at a level commensurate with the threat. The level of protection will be determined by the criticality and sensitivity of the information and the mission supported by the system.	TD P 71-10 VI-1.A, 7	•	•
AD-5	Security requirements shall be reviewed and approved by the management official responsible for security of the AIS or at the installation making the acquisition.	Industry Best Practices	•	•
AD-6	A risk analysis shall be performed to determine the need and type of approved protection techniques for the SBU or classified system.	TD P 71-10, VI-7.A.1.A, 4.a.(3); VI-4.B, 4.a.(4)(cc)	•	•
AD-7	A risk analysis shall be performed prior to the approval of design specifications for new systems or installations.	TD P 71-10, VI-7.A.1.A, 4.a.(1)	•	•
AD-8	A risk analysis shall be performed at periodic intervals commensurate with the sensitivity of the data processed but not to exceed every 5 years if no risk analysis has been performed during that period.	TD P 71-10, VI-7.A.1.A, 4.a.(4)	•	•
AD-9	A risk analysis shall be performed whenever there is a significant change to the installation. A significant modification made to an SBU AIS or network shall require a review to determine the impact on the security of the processed SBU information.	Industry best practices	•	•
AD-10	The results of periodic risk analyses at each installation shall be documented and taken into consideration when certifying sensitive applications processed at the installation.	Industry best practices	•	•
AD-11	Evaluations of the technical and nontechnical security features of the AIS and other safeguards shall be performed in support of the accreditation process.	TD P 71-10, VI-4.B, 3.f.(5)	•	•

DLMR Security Recommendations ADMINISTRATIVE SECURITY				
	Requirement	**Reference**	**SBU**	**C**
AD-12	Security testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the system or network.	TD P 71-10, VI-4.B.1, 6.c	•	•
AD-13	Results of the design reviews and system tests shall be fully documented and maintained in the official agency records.	Industry Best Practices	•	•
AD-14	Security reviews shall be performed at least every 3 years.	OMB A-130, III, 3.a.3	•	•
AD-15	A single summary, chapter, or manual in user documentation shall describe the security features provided by the system, guidelines on their use, and how they interact with one another.	Industry Best Practices	•	•
AD-16	A manual addressed to the security administrator shall present cautions about functions and privileges that shall be controlled when operating a secure system.	Industry Best Practices	•	•
AD-17	The system developer shall provide documentation that describes the test plan, test procedures that show how the security mechanisms were tested and evaluated, and results of the security mechanisms' functional testing.	Industry Best Practices	•	•
AD-18	System security plan documentation shall be prepared for every sensitive system.	FBI ADPT Security Policy; OMB A-130, III, 3.a.2	•	•
AD-19	Security plans shall be reviewed annually.	TD P 71-10, VI-4.B, 4.a.(4)(bb)	•	•
AD-20	Sensitive security documentation shall be kept in a secured area.	Industry Best Practices	•	•
AD-21	A written directive establishes procedures for secure handling and storage for radio transmission and emergency telephone conversation recordings and criteria and procedures for reviewing recorded conversations. (Access to secure recordings should be limited and available only through a specific procedural method.)	CALEA 81.2.8.b, 81.2.8.c	•	•
CONTINGENCY PLANS				
AD-22	Disaster recovery and contingency plans shall be developed for systems processing SBU data.	TD P 71-10, VI-4.B, 4.a.(4)(dd)	•	•
AD-23	Contingency plans shall be tested for the capability to continue providing service within a system based on the needs and priorities of the participants of the system.	OMB A-130, III, 3.a.2.e	•	•
AD-24	AIS contingency plans shall provide details of arrangements made to continue processing, the location of off-premise storage, the location of the alternate processing facility(ies), and other essential information.	Industry Best Practices	•	•
AD-25	A complete copy of each AIS contingency plan shall be stored and maintained in the off-premise storage facility for that AIS facility.	Industry Best Practices	•	•

DLMR Security Recommendations ADMINISTRATIVE SECURITY				
	Requirement	**Reference**	**SBU**	**C**
AD-26	Security measures for the communications center are in place to provide for back-up resources.	CALEA 81.3.1.c	•	•
AD-27	The radio system shall recognize the failure of any repeaters and adjust accordingly.	TIA TSB PN 3594.3.6	•	•
AD-28	Mobiles and portables shall be designed to continue to operate in the event of the loss of trunking service and to provide an additional layer of redundancy.	TIA TSB PN 3594.3.6	•	•
AD-29	The agency has 24-hour two-way radio capability, providing continuous communications between the communications center and officers on duty.	CALEA 81.2.3	•	•
AD-30	Adequate alternate paths shall be available to transport information.	Industry Best Practices	•	•
AD-31	The agency has an alternate source of electrical power that is sufficient to ensure continued operation of emergency communication equipment in the event of the failure of the primary power source. A documented inspection and test of the alternate power source is completed weekly.	CALEA 81.3.2	•	•
SECURITY AWARENESS AND TRAINING				
AD-32	Security training shall be provided to all personnel who manage, use, or operate radio communications components before they perform their jobs.	TD P 71-10, VI-8.A, 4.a.b.c; FBI ADPT Security Policy	•	•
AD-33	Periodic (though at least annual) refresher training shall be provided to each group of users.	TD P 71-10, VI-4B, 3.i	•	•
AD-34	If passwords are selected as the authentication mechanism for a system, users shall be briefed on the following at the time of password issuance: • Password classification and exclusiveness • Measures to safeguard “sensitive” passwords • Prohibitions against disclosing passwords to other personnel • Responsibilities for notifying the security officer of password misuse • Password change procedures.	FBI ADPT Security Policy	•	•
CONFIGURATION MANAGEMENT				
AD-35	Configuration control shall begin in the earliest stages of the design and development of the system or network and extend over the full life of the configuration items included in the design and development stages.	TD P 71-10, VI-7.A.1.B, 4.a	•	•

DLMR Security Recommendations ADMINISTRATIVE SECURITY				
	Requirement	**Reference**	**SBU**	**C**
AD-36	A configuration management system shall be in place that maintains control of changes to any security-related hardware or changes of any line of source or object code of the security-related software. The system shall record by whom, for what reason, and when the change is made.	TD P 71-10, VI-4.A.1 (TD P 85-07, 27, 52)	•	•
AD-37	Every change made to documentation, hardware, and software/firmware shall be reviewed and approved by the security officer.	TD P 71-10, VI-7.A.1.B, 4.b.(2)	•	•
SOFTWARE/DATA SECURITY				
AD-38	New software shall be backed up immediately, retaining the original distribution diskettes in a safe and secure location. Original diskettes shall be write-protected prior to making backup copies.	TD P 71-10, VI-5.A, Attachment, 3	•	•
AD-39	Only newly formatted diskettes shall be used for copying software for backup storage.	TD P 71-10, VI-5.A, Attachment, 3	•	•
AD-40	Backup of data and applications on the file server shall be performed daily on an incremental basis, with a full backup performed weekly. These backups shall be stored in a secure off-site environment.	Industry Best Practices	•	•
AD-41	Damaged software programs shall be restored from the original diskettes, not from regular backups.	TD P 71-10, VI-5.A, Attachment, 3	•	•
AD-42	Only new media shall be used for making copies for distribution.	TD P 71-10, VI-5.A, Attachment, 4	•	•
AD-43	A purge shall be completed after a final overwrite is made using unclassified data.	TD P 71-10, VI-4.F, Attachment, 1.a	•	•
AD-44	Media shall be purged before submitting it for destruction.	TD P 71-10, VI-4.F, Attachment, 1.c	•	•
AD-45	Degaussing with an approved degausser shall be the only method acceptable for purging classified media.	TD P 71-10, VI-4.F, Attachment, 2.a	•	•
AD-46	Overwrite software shall be protected at the level of the media it purges. The overwrite software shall be protected from unauthorized modification.	TD P 71-10, VI-4.F, Attachment, 2.e	•	•
AD-47	Magnetic media shall be physically controlled and safeguarded in a secure manner until destruction of the media or execution of sanitation procedures are approved.	TD P 71-10, VI-4.A.1 (TD P 85-07, 19, 29)	•	•
AD-48	Virus prevention measures commensurate with the level of risk identified in the risk analysis shall be employed to protect the integrity of the software/data.	FBI ADPT Security Policy	•	•
PERSONNEL SECURITY				

DLMR Security Recommendations ADMINISTRATIVE SECURITY				
	Requirement	**Reference**	**SBU**	**C**
AD-49	Individuals who are authorized to bypass significant technical and operational security controls of the system shall be screened.	OMB A-130, III, 3.a.2.c	•	•
AD-50	Each request for access to the sensitive and classified systems shall be individually reviewed and submitted in writing to appropriate personnel for need-to-know criteria and for personnel security clearance status.	FBI ADPT Security Policy	•	•
AD-51	For the multilevel mode of operation, personnel operating AIS equipment at the central site shall have security clearances and have appropriate need-to-know approvals for the data processed in the AIS.	TD P 71-10, VI-4.A.1 (TD P 85-07, 25, 45)		•
AD-52	For the multilevel mode of operation, people accessing the system via local terminals or at remote locations shall have security clearances for the data processed in the AIS. They also shall have appropriate need-to-know only for the data to be accessible from local terminals or remote locations.	TD P 71-10, VI-4.A.1 (TD P 85-07, 25, 45)		•
AD-53	All routine on-site maintenance functions performed by hardware and systems software specialists shall be performed by personnel who have been cleared at the highest level of information the system has been accredited to process; however, these personnel shall be authorized access to only the information/processes required to perform their maintenance tasks.	TD P 71-10, VI-4.A.1 (TD P 85-07, 25, 46)	•	•
AD-54	Personnel applying for critical sensitive positions shall undergo a preplacement background investigation.	TD 85-02, 39, 3-406	•	•

APPENDIX C—PHYSICAL SECURITY GUIDELINES

DLMR Security Recommendations PHYSICAL SECURITY				
	Requirement	**Reference**	**SBU**	**C**
PH-1	The facility housing terminals and communication components shall be protected by appropriate security measures.	TD P 71-10 VI-4.A.1 (TD P 85-07, 24, 44)	•	•
PH-2	Logs containing information on physical access to the facility shall be maintained and retained for a minimum of 2 years.	TD P 71-10, VI-6.B.3, 4.e	•	•
PH-3	Visitors shall wear badges at all time while in the facility.	Industry Best Practices	•	•
PH-4	Escorts shall be provided for unauthorized individuals at all times. Escorts shall have authorization for access to all areas of the facility.	TD P 71-10, VI-6.B.3, 4.f; FBI ADPT Security Policy	•	•
PH-5	The computer room shall be protected by security control mechanisms (e.g., electronic access device, cipher combination).	Industry Best Practices	•	•
PH-6	The computer room shall be locked at all times when authorized personnel are not present.	TD P 71-10, VI-6.B.3., 4.b	•	•
PH-7	The telecommunications room housing network communication lines shall be secured with locking devices at all times to prevent unauthorized intrusion.	Industry Best Practices	•	•
PH-8	Unescorted entry to either the central computer facility or a remote terminal area shall be controlled and limited to personnel authorized to use the system.	Industry Best Practices	•	•
PH-9	Logs shall be required for recording all physical access to the computer room by unauthorized individuals (e.g., vendor maintenance and local telephone company personnel).	TD P 71-10, VI-6.B.3., 4.e	•	•
PH-10	Logs containing information on physical access to the computer room shall be maintained and retained for a minimum of 2 years.	TD P 71-10, VI-6.B.3, 4.e	•	•
PH-11	The cipher combination shall be protected by shielding the locking mechanism against observation by unauthorized personnel.	TD P 71-10, VI-6.B.3, 4.b(2)	•	•
PH-12	Cipher locks shall have key overrides, and combinations shall be changed at least once every 6 months; when anyone with the current combination resigns or transfers; or when an attempt to compromise the combination (either successful or unsuccessful) is made.	TD P 71-10, VI-6.B.3, 4.b(2)	•	•
PH-13	File servers shall be located in areas where access is restricted.	TD P 71-10, VI-5.A, Attachment, 5	•	•

DLMR Security Recommendations PHYSICAL SECURITY				
	Requirement	**Reference**	**SBU**	**C**
PH-14	Location and use of handheld fire extinguishers shall be maintained and inspected in accordance with the National Fire Protection Association, Number 10, Maintenance and Use of Portable Fire Extinguishers. They shall be immediately available to personnel and shall be clearly marked.	FBI ADPT Security Policy	•	•
PH-15	Uninterruptible power source systems and emergency generators shall be tested and properly maintained.	FBI ADPT Security Policy	•	•
PH-16	Smoke detectors, both above and below raised flooring, shall be tested and properly maintained.	FBI ADPT Security Policy	•	•
PH-17	Security measures for the communications center are in place to limit access to authorized personnel.	CALEA 81.3.1.a	•	•
PH-18	Security measures for the communications center are in place to protect equipment.	CALEA 81.3.1.b	•	•
PH-19	Security measures for the communications center are in place to provide security for transmission lines, antennas, and power sources.	CALEA 81.3.1.d	•	•

APPENDIX D—COMPUTER SECURITY GUIDELINES

DLMR Security Recommendations COMPUTER SECURITY(COMPUSEC)				
Requirement		**Reference**	**SBU**	**C**
AUTHENTICATION				
Portable/Mobile Radio & Mobile Data Terminal				
CS-1	The system shall allow the authentication of communication partners.	TETRA 2.22, 6.2	•	•
CS-2	The network shall be able to authenticate mobiles and portables.	TETRA 2.22 6.2 R-2.10.1	•	•
CS-3	Portables and mobiles shall authenticate users to prevent misuse.	TETRA 2.22 6.2 0-2.11, R-2.11.1; TIA TSB PN 3594 4.5.3.21	•	•
CS-4	A radio shall have an Electronic Serial Number (ESN) embedded into the radio and the radio shall respond to ESN inquiries.	TIA/EIA TSB 102-A 5.9.4; TIA TSB PN 3594 3.8.1.3	·	·
Computer-Based Network Components				
CS-5	Source and destination equipment shall be authenticated prior to any configuration or accounting management actions.	TIA/EIA TSB 102-A 5.9.3	·	·
CS-6	Group number (talk group) reassignments shall require authentication.	TETRA 2.22 6.2 R-2.5.3	.	.
CS-7	Dispatcher shall receive reports on authentication failures of users.	TETRA 2.22 6.2 R-2.4.2	.	.
CS-8	Terminal shall authenticate network entities.	TETRA 2.22 6.2 R-2.8.1	.	.
CS-9	Remote change of parameters in the mobile shall require authentication.	TETRA 2.22 6.2 R-2.5.4	.	.
CS-10	The system shall require users to identify themselves and provide some proof that they are who they say they are (e.g., userID and password).	TD P 71-10, VI-4.B.1, 6.b.(1); TIA TSB PN 3594 4.5.3.21	•	•
CS-11	A password shall not be shared by multiple users.	TD P 71-10, VI-4.E.1, 5.a	•	•
CS-12	The system shall store passwords in a one-way encrypted form.	TD P 71-10, VI-4.E.1, 5.c	•	•
CS-13	The system shall automatically suppress or fully blot out the clear-text representation of the password on the data entry device.	TD P 71-10, VI-4.E.1, 5.d	•	•
CS-14	The system shall block any demonstration of password length (e.g., the cursor shall not move upon input).	TD P 71-10, VI-4.E.1, 5.d	•	•

DLMR Security Recommendations COMPUTER SECURITY(COMPUSEC)				
	Requirement	Reference	SBU	C
CS-15	The system, by default, shall not allow null passwords during normal operation.	TD P 71-10, VI-4.E.1, 5.e	•	•
CS-16	The system shall provide a mechanism to allow passwords to be user-changeable.	TD P 71-10, VI-4.E.1, 5.f	•	•
CS-17	The system shall enforce password aging on a per-user basis (e.g., every 90 days). After the password aging threshold has been reached, the password shall no longer be valid and shall require action by the security officer to reset the password.	TD P 71-10, VI-4.E.1, 5.g	•	•
CS-18	The system shall provide a mechanism that notifies the user to change their password.	TD P 71-10, VI-4.E.1, 5.h	•	•
CS-19	Passwords shall not be reusable by the same individual for a period of time specified by the security officer.	TD P 71-10, VI-4.E.1, 5.i	•	•
CS-20	The system shall provide a method of ensuring the complexity of user-entered passwords (e.g., eight characters minimum length).	TD P 71-10, VI-4.E.1, 5.j	•	•
CS-21	As soon as the system has been installed, all vendor supplied passwords, including those for software packages and maintenance accounts, shall be changed.	TD P 71-10, VI-4.E.1, 5.l	•	•
CS-22	Users shall log out when they leave terminals, workstations, and networked personal computers unattended.	TD P 71-10, VI-4.E.1, 5.m	•	•
CS-23	Each individual user (or processors acting in the user's behalf) shall be identified and authenticated by the user AIS when requesting access to another host AIS on a network.	TD P 71-10, VI-4.A.1	•	•
CS-24	The system shall lock out an interactive session after an interval of user inactivity not to exceed thirty minutes.	FBI ADPT Security Policy	•	•
CS-25	User accounts that have been inactive for over 90 days shall be suspended.	FBI ADPT Security Policy	•	•
CS-26	User accounts that have been inactive for the network administrator-specified time period shall be deleted.	Industry Best Practices	•	•
CS-27	User accounts shall be immediately removed when that user no longer requires access to the system.	TD P 71-10, VI-4.E.1, 5.f	•	•
CS-28	Password distribution methods shall be provided protection equivalent to the level of information the passwords protect.	FBI ADPT Security Policy	•	•
CS-29	User access is prohibited after a specific number of invalid login attempts (e.g., three times).	FIPS Pub 112	•	•
CS-30	Initial passwords assigned by a system administrator shall be changed immediately.	Industry Best Practices	•	•
CS-31	Administrator account shall not be shared by numerous individuals.	Industry Best Practices	•	•

Requirement		Reference	SBU	C
ACCESS CONTROL				
Portable/Mobile Radio & Mobile Data Terminal				
CS-32	Personal information shall be transmitted in a secure manner.	TETRA 2.22 6.5 R-5.1.2	•	•
CS-33	Radio resources shall be protected against unauthorized use.	TETRA 2.22 6.8 R-8.1.2	•	•
CS-34	Disabled radios shall only be reactivated through the enable command or reprogramming.	TIA TSB PN 3594 4.5.3.26	•	•
CS-35	Radios that receive regrouping instructions shall not automatically activate the instructions until an activation message is sent.	TIA TSB PN 3594 4.5.3.27	•	•
CS-36	Stolen or lost mobiles shall be protected against misuse.	TETRA 2.22 6.8 R-8.5.1	•	•
Computer-based Network Components				
CS-37	Privileges of monitoring traffic between mobile radio systems shall be assigned only to authorized personnel (e.g., organizational managers, dispatchers).	TETRA 2.22 6.7	•	•
CS-38	Access to databases shall be restricted.	TETRA 2.22 6.8 R-8.1.3	•	•
CS-39	The system security features shall have the technical ability to restrict the user's access to only that information that is necessary for operations.	FBI ADPT Policy	•	•
CS-40	The system shall be configured to protect resources from unauthorized access.	FBI ADPT Policy	•	•
CS-41	The individual who requires access shall have the need-to-know, i.e., access to the information is an operational necessity.	FBI ADPT Policy	•	•
CS-42	System users shall be restricted to only those privileges necessary to perform assigned tasks.	FBI ADPT Policy	•	•
CS-43	Operating files and other executable files shall employ access controls.	TD P 71-10, VI-5.A, Attachment, 5	•	•
CS-44	Improved access control and monitoring shall be implemented for those AIS that permit direct access to centralized databases and processing services from remote locations.	TD P 71-10, VI-4.A, 7	•	•
CS-45	Access permission to an object (e.g., files and programs) shall only be assigned by authorized users.	Industry Best Practices	•	•
CS-46	The AISs shall provide adequate protection (e.g., mandatory access protection) to restrict users' access to the portion(s) of the classified information processed by the AIS for which they are cleared and have a need-to-know.	TD P 71-10, VI-4.A.1 (TD P 85-07, 29, 54.c)		•

DLMR Security Recommendations COMPUTER SECURITY(COMPUSEC)				
	Requirement	**Reference**	**SBU**	**C**
CS-47	If a network and all its connected AIS operate at the system-high or multilevel mode, means shall be provided to establish a session security parameter (e.g., Confidential, Secret, Top Secret) at the beginning of each work session.	TD P 71-10, VI-4.A.1 (TD P 85-07, 43, 43)		•
CS-48	The system shall, by default, mark sensitivity labels that properly represent the highest classification and all appropriate dissemination caveats of the information processed.	TD P 71-10, VI-4.A.1 (TD P 85-07, 21, 34)		•
CS-49	Controls for local area networks shall be established that prevent anyone except authorized staff from loading software on file servers.	TD P 71-10, VI-5.A, Attachment, 5	•	•
CS-50	A local area network file server shall never be used as a workstation.	TD P 71-10, VI-5.A, Attachment, 8	•	•
CS-51	Access to the network file server shall be restricted to authorized maintenance personnel, network operators, and authorized vendors who maintain the network system.	Industry Best Practices	•	•
CS-52	For each AIS connected to a network, authentication data shall be maintained for every user. This authentication data shall be protected so that it cannot be accessed by an unauthorized user.	TD P 71-10, VI-4.A.1 (TD P 85-07, 44, 47)	•	•
CS-53	Network management messages shall be protected against unauthorized access via recording and replay of the messages (spoofing).	TIA/EIA TSB 102-A 5.9.3; TIA TSB PN 3594 4.9.3	•	•
CS-54	Mobile registration data shall be protected against unauthorized eavesdropping.	TIA/EIA TSB 102-A 5.9.3; TIA TSB PN 3594 4.8.3.1.2	•	•
CS-55	Access to configuration/network management shall be restricted.	TETRA 2.22 6.8 R-8.1.5	•	•
CS-56	For a network transmitting or receiving classified data, security parameters shall be attached to all messages on the network by either the subscriber system or the network interface component, and their integrity shall be assured.	TD P 71-10, VI-4.A.1 (TD P 85-07, 45, 56)	•	•
CS-57	The network shall maintain a domain for its own execution that protects it from external interference and tampering.	Industry Best Practices	•	•
Dial-up Controls				
CS-58	All dial-up access to sensitive information shall be protected with appropriate devices or techniques that provide explicit user identification and authentication, and audit trails.	TD P 71-10, VI-4.C.2, 2.a	•	•
CS-59	Access control in the form of well-administered user name and authentication shall be established for each user having dial-in access.	TD P 71-10, VI-4.C.2, 4.a	•	•
CS-60	Modem connections shall be terminated after three failed login attempts or a specified interval with no login. User accounts shall be disabled after three failed login attempts.	Industry Best Practices	•	•

DLMR Security Recommendations COMPUTER SECURITY(COMPUSEC)				
	Requirement	**Reference**	**SBU**	**C**
CS-61	Access restrictions shall be used based on time, date, user, and group to protect network resources and services.	Industry Best Practices	•	•
	AUDIT			
CS-62	Each AIS shall provide the capability to associate an individual user's identity with all auditable actions taken by the individual.	TD P 71-10, VI-4.A.1 (TD P 85-07, 44, 50)	•	•
CS-63	Audit logs shall be retained according to a specified retention period.	FBI ADPT Security Policy	•	•
CS-64	Auditing shall be configured to capture security relevant events.	FBI ADPT Security Policy; TIA TSB PN 3594 4.9.2	•	•
CS-65	Each audit event shall contain the user identification and information relevant to the event (e.g., data and time of the event, type of event, and the success or failure of the event).	FBI ADPT Security Policy; TIA TSB PN 3594 4.9.2, 4.5.3.22	•	•
CS-66	Audit trails shall be reviewed at least once a week.	FBI ADPT Security Policy	•	•
CS-67	Reviewing audit data shall be restricted to designated individuals who are authorized for audit data.	TD P 71-10, VI-4.B.1, 6.b.(2)	•	•
CS-68	Audit trails of network activities shall include at a minimum a record of each action together with appropriate identification parameters, a record of the starting and ending times of each connection, a record of any exceptional conditions detected during the transactions between two (or more) subscribers, and such information as is necessary to allow association of the network activities with corresponding user audit trails and records.	TD P 71-10, VI-4.A.1 (TD P 85-07, 42, 33)	•	•
CS-69	The system shall protect the audit data from destruction.	Industry Best Practices	•	•
CS-70	A means of detecting intrusions and jamming shall be provided.	TETRA 2.22 6.9 R-9.1.3, R-9.1.4	•	•
	OBJECT REUSE			
CS-71	When a storage object (e.g., core area, disk file) is initially assigned, allocated, or reallocated to a system user, all authorization to the information contained within the storage object shall be cleared.	TD P 71-10, VI-4.B.1, 6.b.(4)	•	•
CS-72	No information produced by a prior subject's actions shall be available to any subject that obtains access to an object that has been released back to the system.	Industry Best Practices	•	•

APPENDIX E—COMMUNICATIONS SECURITY GUIDELINES

DLMR Security Recommendations COMMUNICATIONS SECURITY (COMSEC)				
Requirement		**Reference**	**SBU**	**C**
TRANSMISSION SECURITY				
CM-1	Radio channels shall be protected against jamming.	TETRA 2.22 6.8 R-8.1.6	•	•
CM-2	Radio transmissions shall be protected from unauthorized interception.	Industry Best Practices	•	•
CM-3	Replay for voice shall be prevented.	TETRA 2.22 6.4 R-4.4.3	•	•
ENCRYPTION				
General				
CM-4	System shall ensure traffic flow confidentiality to prevent disclosure of information that can be inferred from observing traffic patterns even in the presence of encryption of the message contents.	TETRA 2.22 6.6	•	•
CM-5	Cryptographic-based security systems used by federal agencies to protect sensitive but unclassified information within telecommunications systems (including voice systems) shall be validated.	FIPS 140-1	•	•
CM-6	Information transported from any point in a radio communication shall be exactly the same in content as the data transported.	Industry Best Practices	•	•
CM-7	User identity shall not be exposed at the air interface.	TETRA 2.22 6.5 R-5.5.1	•	•
CM-8	Location information shall not be exposed to network provider.	TETRA 2.22 6.5 R-5.6.1	•	•
CM-9	Control and management information shall be encrypted within the fixed network.	TETRA 2.22 6.3 R-3.1.2	•	•
CM-10	Integrity check of the control and management information shall be provided within the fixed network.	TETRA 2.22 6.4 R-4.1.2	•	•
CM-11	Integrity check of the control channel shall be provided at the air interface.	TETRA 2.22 6.4 R-4.1.1	•	•
CM-12	Integrity check of the user channel shall be provided at the air interface.	TETRA 2.22 6.4 R-4.2.1	•	•
CM-13	All encryption capable equipment shall be designed such that the encryption device can be physically secured when unattended or not in use.	TIA/EIA TSB 102-A 5.9.1.6; TIA TSB PN 3594 3.8.1.2	•	•
CM-14	No system function shall be designed to require encryption facilities within unattended RF subsystem components (e.g., base station). Consequently, all functions related to infrastructure signaling shall be carried out in the unencrypted mode.	TIA/EIA TSB 102-A 5.9.1.6; TIA TSB PN 3594 3.8.1.1.4	•	•

Requirement		Reference	SBU	C
Traffic Channel				
CM-15	The multilevel system shall provide up to four levels of encryption with compatible modes of operation and shall provide the same functions associated with clear (unencrypted digital) operation.	TIA/EIA TSB 102-A 5.9.1.1	·	•
CM-16	Identical services and facilities in the encrypted mode of operation shall be provided both for conventional and trunked modes of operation.	TIA/EIA TSB 102-A 5.9.1.1	•	•
CM-17	An end-to-end encrypted service shall be provided for digital voice and data traffic, using a nonencrypted control channel, and shall allow for the optional encryption of certain control channel functions.	TIA/EIA TSB 102-A 5.9.1.1; TIA TSB PN 3594 3.8.1.1.1	•	•
CM-18	Multiple types of encryption shall be employed simultaneously on the same RF subsystem.	TIA/EIA TSB 102-A 5.9.1.1	•	•
CM-19	Circuit switched reliable data, packet switched confirmed delivery, and packet switched unconfirmed delivery data shall be optionally provided as encrypted services.	TIA/EIA TSB 102-A 5.9.1.2	•	•
Broadcast, Group and Individual Voice				
CM-20	All voice calls shall be provided with a user-selectable voice encryption facility.	TIA/EIA TSB 102-A 5.9.1.3.1; TIA TSB PN 3594	•	•
CM-21	Call addressing shall be supported in either clear or encrypted form, allowing source, destination, and talkgroup IDs to be cryptographically protected if required.	TIA/EIA TSB 102-A 5.9.1.3.1	•	•
CM-22	All signaling shall be carried out on an end-to-end basis when using encrypted IDs.	TIA/EIA TSB 102-A 5.9.1.3.1	•	•
CM-23	All voice calls shall support emergency signaling, scanning, and radio unit monitoring facilities for both clear and secure traffic.	TIA/EIA TSB 102-A 5.9.1.3.1	•	•
CM-24	The data transmission system (including data headers, terminator blocks, acknowledgements and source and destination addresses) shall not be encrypted, whether the service itself is encrypted or not.	TIA/EIA TSB 102-A 5.9.1.3.2	•	•
Encryption Performance				
CM-25	The algorithm performance shall be as defined for the FIPS 46 Data Encryption Standard (DES) for Type 3 systems.	TIA/EIA TSB 102-A 5.9.1.4.1; TIA TSB PN 3594 3.8.1.1.2.1	•	

DLMR Security Recommendations COMMUNICATIONS SECURITY (COMSEC)				
Requirement		**Reference**	**SBU**	**C**
CM-26	The encryption system shall provide for at least 8 crypto keys within each encrypted equipment and shall provide for a minimum of 4 active-traffic keys.	TIA/EIA TSB 102-A 5.9.1.5; TIA TSB PN 3594 3.8.1.1.3	•	
CM-27	The common air interface shall be capable of transporting key variables of up to 72 bits in length.	TIA/EIA TSB 102-A 5.9.1.5	•	
CM-28	Encrypted services shall be provided as end-to-end functions between communicating handheld or mobile radios, consoles, or compatible RF subsystem gateway interfaces.	TIA/EIA TSB 102-A 5.9.1.6; TIA TSB PN 3594 3.8.1.1.4	•	
TEMPEST				
CM-29	Encryption capable equipment shall be designed to meet the TEMPEST requirements appropriate to the level of algorithm employed.	TIA/EIA TSB 102-A 5.9.1.7		•
CM-30	Type 1 systems shall implement TEMPEST requirements specified by the Federal Government.	TIA/EIA TSB 102-A 5.9.1.7; TIA TSB PN 3594?		•
Control Channel Signaling				
CM-31	The control channel shall be optionally encrypted (a standard option) based on a packet by packet basis. A marker shall be transmitted in the clear section of the message packet to indicate an encrypted packet to all radio units active on the control channel.	TIA/EIA TSB 102-A 5.9.2	•	•
CM-32	No control channel encryption device shall be located at a remote unattended base station location.	TIA/EIA TSB 102-A 5.9.2	•	•
CM-33	Authentication and synchronization mechanisms shall allow for possible delays between base station and RF subsystem control.	TIA/EIA TSB 102-A 5.9.2	•	•
CM-34	The system shall detect and alert the system operator of the occurrence of jamming and shall have the ability to change control channel either automatically or manually from a network management terminal.	TIA/EIA TSB 102-A 5.9.2	•	•
KEY MANAGEMENT				
General				
CM-35	All classified transmissions shall be secured with National Security Agency (NSA) approved encryption devices and techniques.	TD P 71-10, VI-4.A.1 (TD P 85-07, 24, 41); 31 CFR PART 2, 60, 2.29		•
CM-36	Secret keys and private keys shall be protected from unauthorized disclosure, modification, and substitution. Public keys shall be protected against unauthorized modification and substitution.	FIPS Pub 140-1	•	

DLMR Security Recommendations
COMMUNICATIONS SECURITY (COMSEC)

Requirement		Reference	SBU	C
CM-37	When a random number generator is used in the key generation process, all values shall be generated randomly or pseudo randomly such that all possible combinations of bits and all possible values are equally likely to be generated.	FIPS Pub 140-1	•	
CM-38	A seed key, if used, shall be entered in the same manner as cryptographic keys.	FIPS Pub 140-1	•	
CM-39	Intermediate key generation states and values shall not be accessible outside the module in plain text or otherwise unprotected form.	FIPS Pub 140-1	•	
CM-40	When encrypted keys or key components are entered, the resulting plain text secret or private keys shall not be displayed.	FIPS Pub 140-1	•	
CM-41	A means shall be provided to ensure that all keys are associated with the correct entities to which the keys are assigned.	FIPS Pub 140-1	•	
CM-42	All key material used for the protection of classified or SBU information shall be generated, distributed, stored, and destroyed in a secure and controlled manner.	TD P 71-10, VI-3.C, 2	•	
CM-43	Written guidelines shall be established in the form of a key management plan for the handling and safeguarding of keying material.	TD P 71-10, VI-3.C, 4.b	•	
CM-44	COMSEC keying material that contains cryptographic information shall bear the designation CRYPTO.	TD P 71-10, VI-3.D.1, E.2	•	
CM-45	Key cards and key lists that are wrapped in protective packaging shall not be opened until 72 hours prior to the effective date; therefore, a page check upon receipt of the material is not authorized.	TD P 71-10, VI-3.D.1, I.2.a	•	
CM-46	Test keying material shall not be opened until it is to be used.	TD P 71-10, VI-3.D.1, I.2.a	•	
CM-47	Key tapes in protective canisters shall not be removed from the canisters for inventory or check purposes. The tape shall be removed only by the users of the material on the effective date.	TD P 71-10, VI-3.D.1, I.2.a	•	
CM-48	COMSEC keying material, both regularly and irregularly superseded, shall be destroyed as soon as possible and shall be destroyed within 12 hours after supersession or use.	TD P 71-10, VI-3.D.1, N.2.b	•	
CM-49	COMSEC material involved in compromised situations shall be destroyed within 72 hours after disposition instructions are received.	TD P 71-10, VI-3.D.1, N.2.b	•	
CM-50	Individuals responsible for the handling of key material (COMSEC Custodian) shall possess knowledge of COMSEC and sufficient authority to perform custodial duties and shall be indoctrinated for cryptographic access.	TD P 71-10, VI-3.D.1, D.1	•	•
Encrypted Radio				
CM-51	All encrypted radios shall be provided with a common key-fill interface.	TIA/EIA TSB 102-A 5.9.1.8.1	•	•

DLMR Security Recommendations COMMUNICATIONS SECURITY (COMSEC)				
Requirement		**Reference**	**SBU**	**C**
CM-52	All equipment using the same encryption device shall use a common key-fill device.	TIA/EIA TSB 102-A 5.9.1.8.1	•	•
CM-53	Encrypted radios shall be provided with a zeroize facility to allow the user to erase encryption keys in an emergency.	TIA/EIA TSB 102-A 5.9.1.8.1	•	•
CM-54	Mobile radios may be provided with a crypto ignition key (CIK) to allow a user to secure an unattended radio by removal of this key.	TIA/EIA TSB 102-A 5.9.1.8.1	•	•
CM-55	Manual fill, zeroize, and CIK facilities may be provided remotely to a mobile radio for ease of access.	TIA/EIA TSB 102-A 5.9.1.8.1	•	•
CM-56	Key variables shall not be extracted from an encrypted radio for use in cloning unfilled equipment.	TIA/EIA TSB 102-A 5.9.1.8.2	•	•
Over the Air Rekeying				
CM-57	The system design shall provide support for over-the-air rekeying (OTAR) of encryption devices.	TIA/EIA TSB 102-A 5.9.1.8.3; TIA TSB PN 3594 3.8.1.1.5.2	•	•
CM-58	OTAR messages shall be encrypted before transmission and shall not be required to provide the RF subsystem with unencrypted address or userID information.	TIA/EIA TSB 102-A 5.9.1.8.3	•	•
CM-59	The key management modules (KMM) shall be transmitted over the CAI using the encrypted data mode as specified in the Project 25 DES Encryption Protocol.	TIA/EIA TSB-102.AACA D.3	•	•
CM-60	All DES Type 3 keys, contained in Type 3 KMMs, shall be 64-bits in length.	TIA/EIA TSB-102.AACA D.4	•	•
CM-61	All keys contained in KMMs shall be encrypted using the DES in the Electronic CodeBook (ECB) Mode. The key used for this encryption process shall be a key encryption key (KEK).	TIA/EIA TSB-102.AACA D.4	•	•
CM-62	KEKs shall only be used to encrypt other keys.	TIA/EIA TSB-102.AACA D.4	•	•
CM-63	The algorithm ID and the key ID fields in the decryption instruction block shall specify the algorithm ID and key ID of the KEKs used to encrypt the keys contained in the sequence of unique key item blocks.	TIA/EIA TSB-102.AACA D.4.1	•	•
CM-64	The DES algorithm shall not use the optional checksum field following the key field.	TIA/EIA TSB-102.AACA D.4.1	•	•
CM-65	Messages specified in TIA/EIA TSB-102.AACA, D.5 shall contain a 7-octet message authentication code (MAC) field.	TIA/EIA TSB-102.AACA D.5	•	•
CM-66	Messages shall be authenticated using the DES in either the 64-bit cipher block chaining (CBC) mode of operation or the 64-bit cipher feedback (CFB) mode of operation as specified in FIPS Pub 81.	TIA/EIA TSB-102.AACA D.5	•	•

DLMR Security Recommendations COMMUNICATIONS SECURITY (COMSEC)				
Requirement		**Reference**	**SBU**	**C**
CM-67	The key used to generate the MAC shall be any transmission encryption key held in common between the originator and destination(s).	TIA/EIA TSB-102.AACA D.5	•	•
CM-68	The TEK used to authenticate messages shall be changed before MNS are duplicated.	TIA/EIA TSB-102.AACA D.5	•	•
CM-69	Key updating shall not be supported by DES Type 3 encryption.	TIA/EIA TSB-102.AACA D.6	•	•
CM-70	Composite and Primitive field definitions for public key encryption messages shall be classified for Type 1 encryption.	TIA/EIA TSB-102.AACA D.7		•
CM-71	Message number processing messages specified in TIA/EIA TSB-102.AACA, D.8 shall contain a 2-octet message number (MN) (if the MN of the received can be determined).	TIA/EIA TSB-102.AACA D.8	•	•
CM-72	The key management facility (KMF) shall assign and keep track of MNs for each individual RSI or group RSI for which it sends a key management module.	TIA/EIA TSB- 102.AACA D.8	•	•
CM-73	The KMF shall increment the destination RSI message for each new message it creates.	TIA/EIA TSB-102.AACA D.8	•	•
CM-74	The mobile radio (MR) shall maintain a MN for its own individual RSI and for each group RSI for which it is a part of in non-volatile memory.	TIA/EIA TSB-102.AACA D.8	•	•
CM-75	The message number period (MNP), a system dependent parameter, chosen by the security system administrator, shall be programmable for all Type 3 devices.	TIA/EIA TSB-102.AACA D.8	•	•
CM-76	A two-octet MN field shall be included for all Type 3 KMMs.	TIA/EIA TSB-102.AACA D.8	•	•