Public Safety Wireless Network

PSWN

# *Security Field Data Collection & Analysis Report*

# *Site #1 800 MHz Analog Trunked Radio System*

**Final**

October 1998

# FOREWORD

This report presented by the Public Safety Wireless Network (PSWN) program documents security issues and candidate recommendations identified during the first of a series of security field data collection and analysis efforts. The primary goals of these efforts and the resulting reports are to raise security awareness and understanding and to help mitigate security risks associated with evolving public safety communications systems.

Questions or comments regarding the information contained in this document should be forwarded to the PSWN Program Management Office (PMO) at 800-565-PSWN. For more information regarding the purpose and goals of the PSWN program, see the PSWN web site at www.pswn.gov.

# TABLE OF CONTENTS

**Page**


**1. INTRODUCTION ..... 1**

1.1 PURPOSE ..... 1
1.2 SCOPE ..... 2
1.3 DOCUMENT ORGANIZATION ..... 2

**2. APPROACH ..... 3**

**3. SYSTEM DESCRIPTION ..... 4**

**4. SYSTEM SECURITY FINDINGS ..... 7**

4.1 SECURITY ISSUES ..... 7
*4.1.1 Scanners Are a Concern ..... 8*
*4.1.2 Primary Channels Transmitted in the Clear ..... 9*
*4.1.3 MDT Transmission Interception is a Concern ..... 10*
*4.1.4 Encryption-Capable Radios Are Not Used in Encrypted Mode ..... 11*
*4.1.5 System Dial-in Capability Could Be Exploited ..... 11*
*4.1.6 Data Integrity Is a Greater Concern Than Data Confidentiality ..... 12*
4.2 BEST SECURITY PRACTICES ..... 13
*4.2.1 System Reliability and Availability Should be Ensured ..... 13*

**5. SUMMARY ..... 14**

Appendix A—Acronyms ..... A-1

# 1. INTRODUCTION

The Public Safety Wireless Network (PSWN) program has deployed case study teams to conduct detailed interviews with managers and users of public safety radio systems in selected regions of the United States. The case study interview guides used by these teams include several security-related questions. The PSWN program also has initiated a number of security-focused data collection and analysis activities. These data collection activities build on the security information gathered through the case studies by collecting more detailed security information at a few selected sites. A *Security Field Data Collection Summary Report* will be prepared at the conclusion of the initial series of security-focused data collection efforts. These efforts support the larger goal of establishing the PSWN program as a valuable information resource and a source of guidance for many aspects of public safety communications.

On October 8, 1997, an Emergency Communications Center (ECC) serving police, fire, and emergency medical services became the first site visited under the security data collection and analysis effort. This report documents the results of that effort. All references to the agency visited have been removed from the report.

When conducting a site visit, the PSWN team uses an internally prepared security data collection plan as a guide to ensure all pertinent information is collected. Site visits provide the PSWN team an opportunity to improve the plan based on lessons learned following each visit. This process ensures the PSWN team requests the latest, most accurate, security relevant information at subsequent site visits.

## 1.1 Purpose

The security field data collection activities will increase understanding of the emerging security issues associated with evolving public safety communications infrastructures. These efforts also will provide insight into the risks associated with the computerization and digitization of those infrastructures as well as the security concerns and needs of the public safety community. In addition, the studies will identify best security practices and measures taken to decrease the risk to public safety radio components and information.

Security field data collection activities support the following goals:

- Identifying the sensitivity levels of data communicated
- Documenting communications infrastructures used, including wireless and wireline connectivities
- Describing existing technical and procedural security controls

- Identifying security concerns, as well as the frequency and nature of known security issues and incidents
- Capturing existing best security practices and security measures.

Additional security issues, concerns, and practices will be documented as data are collected at additional public safety agency sites. Those findings, as well as the findings in this report, may reveal patterns or commonalities in the security of public safety communications. Dissemination of security issues, best practices, and candidate recommendations to the public safety community should provide valuable guidance as the community makes decisions about the security of its systems.

## 1.2 Scope

The security-focused field data collection is intended to gather security-related data on public safety communications infrastructures to enhance the understanding of possible risks to these infrastructures. This report is not an evaluation of the security practices of any particular public safety agency or of public safety communications infrastructures in general. Candidate recommendations are included for each security issue identified in the report. These recommendations and new candidate recommendations will continue to be evaluated during subsequent data collection activities for potential inclusion in a summary report.

## 1.3 Document Organization

This document is divided into the following sections:

- Section 1, Introduction—Presents background, purpose, scope, and document layout.
- Section 2, Approach—Describes the approach used in conducting the security field data collection and analysis.
- Section 3, System Description—Presents a description of the system analyzed and the organization visited.
- Section 4, System Security Findings—Presents issues identified during the data collection effort and any best practices used by the subject organization to secure its system.
- Section 5, Summary—Provides a synopsis of the findings discussed in the previous section and highlights potential security misperceptions.
- Appendix A, Acronyms—Contains a list of acronyms used in this report.

# 2. APPROACH

This section describes the approach used in conducting this security field data collection and analysis effort. Subsequent data collection efforts will follow a similar approach and will be conducted in accordance with a data collection plan containing several security questionnaires. The use of the data collection plan will ensure consistency across site interviews and adequate coverage of security.

**Step 1: Coordinate and prepare for data collection effort**

- Identify personnel for conducting the security data collection effort
- Coordinate the data collection schedule
- Determine which site personnel should be interviewed
- Identify the type of system components at the site for pre-interview research
- Prepare a list of questions for use during the interviews.

**Step 2: Collect system and site data**

- Validate system information collected in Step 1
- Collect more detailed information about the site's system configuration including a system diagram if possible
- Identify current security practices, concerns, and needs.

**Step 3: Research and clarify data gathered from the site**

- Collect data from various sources (e.g., Internet, professional journals) concerning security issues and concerns raised
- Recontact the site, if necessary, to clarify information gathered.

**Step 4: Analyze and document security issues, candidate recommendations, and best practices**

- Describe the security issues raised during data collection
- Provide candidate countermeasure recommendations, as applicable, for security issues
- Document existing best practices at the site
- Consolidate the site data and their analysis into a report.

# 3. SYSTEM DESCRIPTION

The ECC serves as the 9-1-1 emergency reporting center for a county and as the dispatch center for police, fire, and emergency medical service (EMS) units. The center is staffed by approximately 50 trained professional personnel.

The ECC's main communications are supported by a mobile radio system with a third-generation Computer-Aided Dispatch (CAD) system. The ECC system includes a 15-channel 800 Megahertz (MHz) trunked analog radio system using four simulcast transmitter sites. Three of the 15 channels are equipped to support secure communications through a Digital Voice Privacy (DVP) feature. Figure 1 provides an overview of the 800 MHz system and a high-level view of mobile data terminal (MDT) connectivity. The ECC also simulcasts its police and fire department primary channel communications on ultra high frequency (UHF) conventional analog systems. A dedicated system using another UHF frequency is used for MDT traffic. Augmenting the primary center is a backup auxiliary operations center (AOC) maintained at a fire station. In addition, the police department's mobile command post vehicle contains a fully functional communications area with the following equipment:

- Very high frequency (VHF), UHF, and 800 MHz radios
- Computer-aided dispatch terminal
- Scanner monitor radio
- Cellular telephones
- Hardwired telephones and 9-1-1 telephones
- MDT
- Facsimile (FAX) machine and copier.

The system's primary radio frequency (RF) site has primary and backup prime site controllers. The backup prime site controller immediately gains control of the system if the primary controller goes down. The AOC, shown as Remote RF Site #2 in Figure 1, contains a prime site controller in cold standby mode. The AOC is activated if the primary RF site goes down. The cold standby-system's subscriber database is kept current with the primary RF site database to ensure that operations are minimally affected when the AOC assumes control. Uninterruptible power supplies and generator backup power are provided at all RF locations and at the ECC. Each site also contains entry, heat, and smoke alarms that send a notification to the ECC under the appropriate conditions. Access to the ECC is controlled by requiring entrance through two cipher lock enabled doors, remote sites are all physically secured by a combination of locked doors and controlled access to the spaces they occupy (e.g., on the upper floor of an office building).

The ECC is connected to the rest of the 800 MHz communications system by digital microwave radio. Control and management of the 800 MHz radio system are performed by the ECC radio system manager. The radio system manager uses a network management system and system- monitoring software to configure, control, and monitor the system. Both of these systems are hardwired to the primary RF site. In addition, there is dial-in access to a computer to allow the radio system manager to control the radio system remotely when required. Dispatchers can perform dispatch-related control of the radio system from the dispatch console. The simulcast and MDT communications systems are connected to the ECC via conventional analog UHF elements co-located with the 800 MHz system components.

# 4. SYSTEM SECURITY FINDINGS

This section describes the security issues and the best practices identified during the site visit and in subsequent research. It includes a table that maps each security issue to one or more data collection sources.

## 4.1 Security Issues

The security issues described in this section include possible implications or associated risks along with candidate recommendations on mitigating the risks. Table 1 summarizes the identified security issues and the corresponding recommendations. The following subsections provide more details. Table 2 lists the data sources used in identifying the security issues and the best practices.

**Table 1**
**Summary of Security Issues and Candidate Recommendations**

| Section | Security Issue | Candidate Recommendation |
|---|---|---|
| 4.1.1 | Scanners are a concern. | Agencies should be made aware that all conventional or trunked analog unencrypted communications are vulnerable to interception and monitoring using low cost, commercially available radio scanners. |
| 4.1.2 | Primary channels transmitted in the clear. | Agencies with trunked systems that transmit information on a clear conventional analog channel for the benefit of the public or press should establish operating policies that move communications from the clear channel to an encrypted channel (if available) or tactical talk group as soon as possible. Agencies should remain vigilant in identifying incidents in which interception and misuse of unprotected information has jeopardized any operation. |
| 4.1.3 | MDT transmission interception is a concern. | Agencies using MDTs to communicate sensitive information over unencrypted channels should consider employing encryption techniques. |
| 4.1.4 | Encryption-capable radios are not used in encrypted mode. | Agencies should ensure that security mechanisms will not significantly interfere with operations. They should ensure that mechanisms are configured properly and that users receive sufficient training. |
| 4.1.5 | System dial-in capability could be exploited. | Network managers should be made aware of network dial-in vulnerabilities and secure practices (e.g., modem dial-back, token-based authentication, password parameter settings). Security policies should address this remote management and maintenance point of entry. |
| 4.1.6 | Data integrity is a greater concern than data confidentiality. | Data integrity and confidentiality concerns should be considered as the development of comprehensive security requirements and guidelines progresses. |

**Table 2**
**Data Collection Sources**

| Data Collection Source | 4.1.1 | 4.1.2 | 4.1.3 | 4.1.4 | 4.1.5 | 4.1.6 | 4.2.1 |
|---|---|---|---|---|---|---|---|
| Site interview | • | • | • | • | • | • | • |
| ECC web site | | | | | | | • |
| Internet newsgroups | • | | | | | | |
| Scannerists' Internet web sites | | • | | | | | |
| Scannerists' publications | • | | | | | | |
| Public safety publications | | | • | | | | |
| Site/radio system vendor correspondence | | | • | | | | |
| Vendor system documentation | | | | | | | • |

### 4.1.1 Scanners Are a Concern

The use of radio scanners by hobbyists, the public, and the press to listen to public safety communications has existed for some time. In the past, this recognized activity has been of little concern to the public safety community since no harm has resulted to public safety officials. Seizures of computers and radio scanners used by criminal elements to monitor police communications is changing the perception that monitoring public safety communications is a benign activity. Additionally, more detailed information concerning private citizens is being sent over unprotected public safety wireless systems and networks thus supporting the need for some form of protected wireless system. In instances where public safety agencies have installed fully encrypted radio systems or used other technologies (such as trunking) that have prevented the use of radio scanners, the press has challenged the use of these technologies by arguing the public has a right to know.

With the introduction of trunked radio systems, many public safety officials were lulled in a false sense of security with the knowledge that earlier radio scanners could not follow the communications associated with trunked systems. However, multiple vendors have since developed scanners capable of tracking trunked analog communications. Review of various Internet newsgroups has revealed that these products are in use.

In addition, public safety frequencies are readily available on the Internet and through other sources. A scanner newsgroup entry noted that a "National Public Safety Trunked System Frequency Guide" is included with the purchase of a trunking scanner. In addition, a particular newsgroup has published the public safety frequencies for the county in which the ECC is located along with instructions for programming the trunking scanner to monitor specific talkgroups. In another newsgroup, when an individual requested a list of a certain county's Police Department frequencies, the response included the type of land mobile radio (LMR) system used by that department, the type of scanner needed (trunking), and an offer to provide the names of user groups.

Although trunking has not been considered a security feature, it has been perceived as providing an additional level of obscurity for "hiding" communications traffic. Agency personnel had considered their voice communications to be unavailable to the general public because of trunking. Until the development of the trunk-tracking scanners, this perception was correct; average citizens did not have the ability to follow complete, coherent conversations. However, the advent of trunk-tracking scanners has enabled the average citizen to follow such conversations, making the communications available to anyone with the new scanner and knowledge of the appropriate frequencies. A related misconception identified during this data collection is that users perceive the "private call" radio feature, in which two radio users may talk on their own frequency, as being secure. These conversations can be scanned just as readily as any other clear communications.

**Candidate Recommendation:**

Public safety agencies should be made aware that all unencrypted analog communications, voice or data, conventional or trunked, are susceptible to interception and monitoring at any point in a land mobile radio system. Radio users should also be made aware that the "private call" feature does not offer voice privacy or security. Agencies installing digital land mobile radio systems should remain vigilant when permitting unencrypted digital communications on the system. The use of end-to-end encryption can lessen the probability of public safety communications being intercepted by unauthorized personnel.

### 4.1.2 Primary Channels Transmitted in the Clear

The ECC transmits its police and fire department primary channel communications in the clear on a UHF conventional analog system as well as on their trunked 800 MHz analog system. Depending upon the sensitivity and extent of the information being communicated on this channel and the intent of the listener, some degree of security risk may exist for public safety operations and privacy information may be disclosed to unauthorized individuals. For example, the concern was recently raised about the interception and misuse of apartment entry codes transmitted in the clear. To mitigate this potential security issue, public safety personnel have been told to use their MDTs to communicate sensitive information as a secure alternative, although, as described in Section 4.1.3, MDT traffic may also be a vulnerable avenue of communications.

**Candidate Recommendation:**

Public safety radio users should move from the primary channel to a tactical channel as soon as possible to reduce the chance of exposing sensitive communications. However, to ensure the confidentiality of tactical channel communications, encryption should be employed. Agencies should remain vigilant in identifying incidents in which the interception and misuse of any clear information has jeopardized critical missions or endangered citizens.

### 4.1.3 MDT Transmission Interception is a Concern

An individual anonymously posted information on the Internet claiming the ability to convert a proprietary mobile data protocol in order to intercept and interpret mobile data transmissions. They also indicated the possibility of spoofing (i.e., transmit with the appearance of being sent by an authorized user of the system) message data on an MDT network. An MDT.exe C++ software program was posted. An issue of a trade publication documented this Internet posting.

An ECC administrator raised the issue within his agency and with the vendor to determine whether the information was accurate, what concerns the agency should have, what actions could or should be taken, and whether the vendor could provide additional information. The vendor's response basically stated that voice and data wireless transmissions are not immune to hacker attacks. The vendor noted that wireline computer users have confronted the same problem for years. They did, however, downplay the risk of unauthorized MDT interception, noting that the technical sophistication required to send data on a mobile data system would make it unlikely.

An article in a subsequent issue of the trade publication stated that the MDT hacker software works but the packets are unsorted. According to the article, transmission packets are received out of order, so reconstruction of a message may be difficult on a busy system.

The data that are transferred between an MDT and local and national databases are typically unencrypted. For the ECC, data are transmitted on a dedicated, UHF frequency and include the following types of information:

- Driver's license information
- Motor vehicle information
- Local records
- Local criminal information network data
- National Crime Information Center (NCIC) data.

On the basis of the information discussed, it is believed that the current security risk associated with the interception of MDT traffic is likely to be low. However, unencrypted MDT traffic is no more secure than unencrypted voice traffic. As has occurred with the development of trunking scanners, it appears that devices and software will become available to the general public to enable MDT traffic to be easily monitored.

**Candidate Recommendation:**

Agencies using MDTs to communicate sensitive information over unencrypted channels may want to consider employing encryption techniques. It is only a matter of time before methods for monitoring unencrypted MDT traffic are publicly available. In addition, when procuring wireless data services through commercial providers offering "encryption", agencies

should closely examine the type and level of encryption being offered to determine if it is sufficiently secure for their needs. If the algorithm used is not DVP or DES, the encryption scheme may be trivial to break by determined individuals.

### 4.1.4 Encryption-Capable Radios Are Not Used in Encrypted Mode

The agency's vice squad requested and received radios with encryption capability. In addition, system resources were dedicated to support this capability. After some time, the radio system manager observed that the dedicated system resources allocated for use by the vice squad were not being used. When queried, vice squad personnel indicated that the voice quality was degraded when using the radios in the encrypted mode. It was their perception the encrypted radios just "didn't work" as well as those without this capability. Although the vice squad recognized the need to protect their communications, they chose to operate in the clear rather than jeopardize their operations when operating in the encrypted mode.

Many users of analog radio systems complain of poor voice quality when operating in the encrypted mode. Users have also complained of a reduction in range when using encryption. These are known technical issues effecting analog radio systems when encryption is introduced. The impact of these problems can be lessened but not totally eliminated. User confidence can be enhanced through proper training. Although the transition from analog to digital communications may itself introduce some degradation in range and voice quality, the introduction of encryption into digital radio systems should not affect range or voice quality.

**Candidate Recommendation:**

Agencies should ensure that any new security mechanism will allow their personnel to do their jobs in the same way that they do them with current equipment. In addition, an agency should ensure that it receives proper instruction from the vendor and assurance of the proper configuration of mechanisms (based on the agency's security policy, if one exists). Users, in turn, should be trained in the proper use of the security mechanisms.

### 4.1.5 System Dial-in Capability Could Be Exploited

The ECC's dispatch network has a dial-in capability that radio system administrators use for remote administration. The ECC dispatch network includes connectivity to the local area network within the ECC building, a larger wide area network, and remote databases. These interconnections introduce the possibility that intruders who gain access to a host on the network could greatly expand their access by exploiting vulnerabilities.

The telephone number for the dial-in entry point is an unpublished number known only to a few ECC personnel. However, commonly used automated tools called wardialers could exploit this point of entry. Wardialers are used to identify modems among a range of phone numbers. They may be configured to repeatedly attempt to login to a remote computer, once a modem connection is made, using numerous user IDs and a dictionary of possible passwords.

The identification and authentication controls used for this entry point consist of various screen names and passwords. Each screen name has a separate password associated with it. The screen names are the same names that are associated with the screens when they are used on-site. Therefore, limiting the distribution of the password for a particular screen can enforce restriction to certain functions (e.g., menu choices on the screen). The passwords are not strong. They consist of no more than eight letters, and no numbers or special characters are used. In addition, the passwords have not been set to expire and have not been changed since the system was installed 6 years ago. After three unsuccessful login attempts, further attempts are prohibited until 30 seconds has elapsed, a report is generated, and the report is sent to the printer. Such a report could go unnoticed for a day or more because the printer is not frequently checked.

Most significantly, this entry point provides an avenue through which many aspects of the radio system can be modified or deleted. A talkgroup could have its name or membership and its mappings of frequencies to talkgroups modified, and the whole system could be shut down or made unusable by a determined hacker.

**Candidate Recommendation:**

Awareness of the potential vulnerabilities associated with various network access methods should be raised in the public safety community because it is likely that similar remote access "conveniences" exist on other public safety communications networks. Security safeguard options should be considered by network managers to mitigate the risk of such vulnerabilities (e.g., modem dial-back, token-based authentication, password configuration constraints).

### 4.1.6 Data Integrity Is a Greater Concern Than Data Confidentiality

ECC administrators rated data integrity as a higher priority than confidentiality. In other words, the communication of accurate information (i.e., sender identity and the message transmitted are understandable and unchanged from the origination point) is vital to the site's mission-critical operations. Protecting "privacy information" in databases from unauthorized disclosure and protecting that information en route, although important, are considered secondary concerns.

As described in Section 4.1.3, it is possible to intercept MDT transmissions. It is implied in the resource information analyzed that it is also possible to masquerade as an authorized user of an MDT and to construct phony messages. Because there has been no proven ability to adequately intercept messages, and the insertion of phony messages is much more complex and difficult than is implied in the resource material, it appears that the risk of phony messages being inserted into a system is insignificant at this time. However, as an added precaution, the ECC has notified MDT users to be wary of unusual message traffic (for instance, when messages that appear to have originated from specific MDTs but the MDT operators indicate that they did not send the messages).

**Candidate Recommendation:**

The capability of masquerading as an authorized MDT user should continue to be monitored. Additional methods of providing data integrity for MDT transmissions should be investigated.

## 4.2 Best Security Practices

The "best security practices" presented in this section include concepts, designs, and procedures that appear to be reasonable methods of mitigating security risks to public safety communications infrastructures. Each best practice includes a description of the practice and the threat(s) that it counters.

### 4.2.1 System Reliability and Availability Should be Ensured

System availability and reliability can be increased through the use of infrastructure redundancy, the technical ability to continue communications in a degraded state, and contingency plans and procedures.

Infrastructure redundancy and the ability to continue communications in a degraded state are often linked together and provided by many vendors' radio systems For example, the ECC's hot standby prime controller provides redundancy of equipment that enables the system to operate normally even if the prime controller fails. Its backup cold standby controller at the AOC provides for degraded operations by performing limited trunking operations (with the other two sites reverting to local failsoft operations) in case both the main and hot prime controllers fail. The multiple consoles in the ECC also act as redundant equipment with the dispatching console at the AOC acting as a degraded state option if equipment failures are encountered.

The preparation and use of contingency plans and procedures ensures that public safety personnel remain proficient in providing service under adverse conditions. The ECC's contingency plan covers both localized equipment failures and environmental conditions requiring relocation of emergency communications. As described in the previous paragraph most local equipment failures are handled by the vendors' equipment and design. For evironmental conditions, the ECC, exercises its AOC on a monthly basis to ensure its viability and ECC personnel's familiarity with their roles and responsibilities.

# 5. SUMMARY

This section provides a synopsis of the security issues presented in Section 4, highlighting potential security misperceptions.

The security issues identified during the first site visit and through subsequent information gathering are summarized as follows:

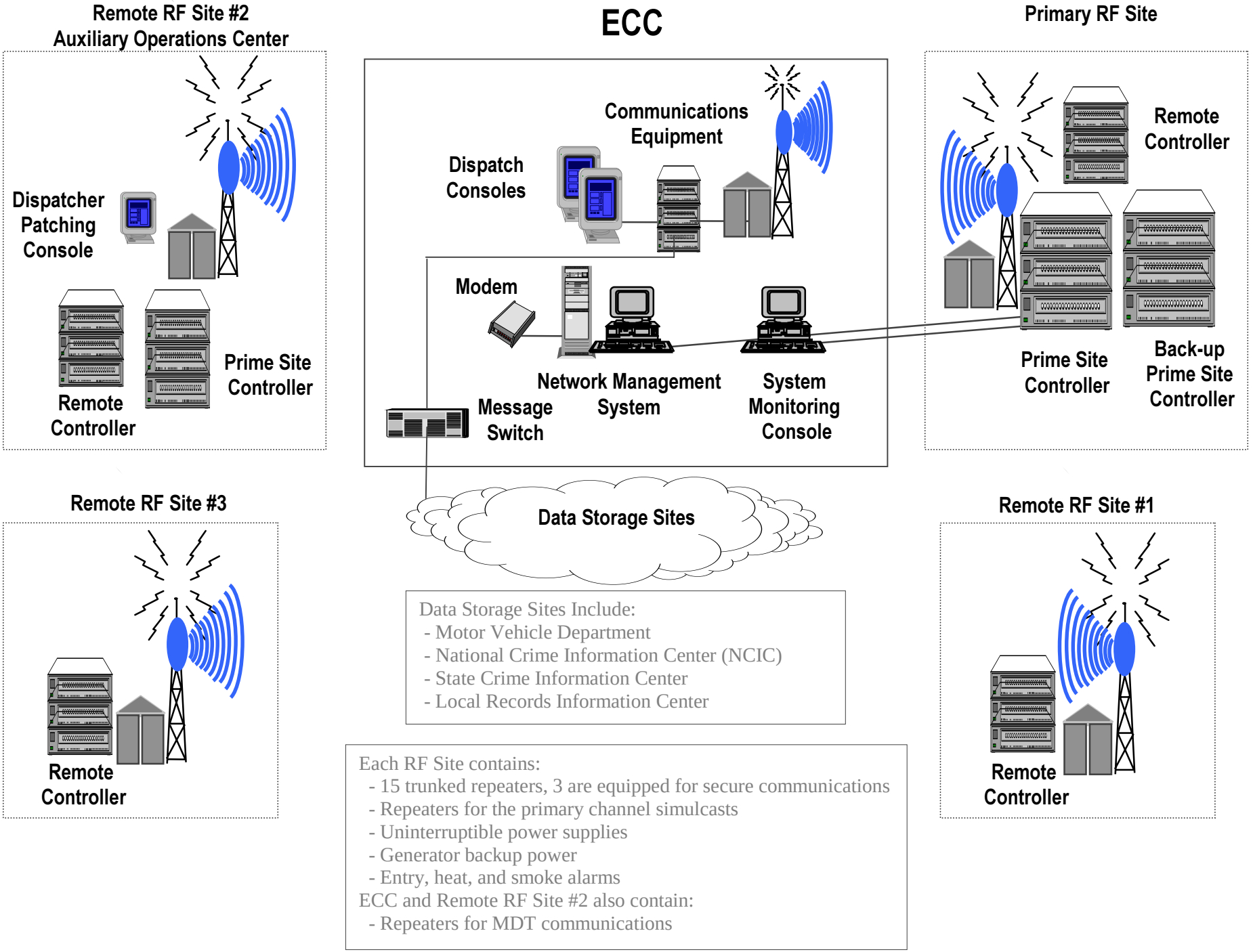
- Unencrypted communications are vulnerable to interception and monitoring using low cost, commercially available radio scanners. Neither trunking nor the use of the "private call" feature provide any reliable degree of security.
- MDT transmission conversion is possible and would allow a hacker to determine the contents of MDT traffic.
- Encryption capable radios are not used in the encrypted mode, negating the value of the encryption.
- The dial-in capability of the system and the lack of added security measures for controlling that connection, leave the system open to potential exploitation.
- Data integrity (i.e., ensuring that the data and the identity of the sender of a transmission have been unaltered) is more important than ensuring the privacy of the data.

Two of the security issues identify areas in which potential misperceptions of security may exist. The first issue concerns a possible perception that trunking provides a level of security for communications. As stated in Section 4.1.1, trunk-tracking scanners are readily available. The second issue involves the perception that mobile data transmissions are secure. Although current indications are that discerning the content of MDT messages is not easy, the ability does exist to convert the content of such messages and eventually a method will be developed to make that content understandable. Therefore, MDT transmissions should not be considered secure. Security misperceptions will continue to be tracked and documented in subsequent reports.

# APPENDIX A

## Acronyms

| | |
|---|---|
| AOC | Auxiliary Operations Center |
| CAD | Computer Aided Dispatch |
| DVP | Digital Voice Privacy |
| ECC | Emergency Communications Center |
| EMS | Emergency Medical Service |
| FAX | Facsimile |
| LMR | Land Mobile Radio |
| MDT | Mobile Data Terminal |
| MHz | Megahertz |
| PMO | Program Management Office |
| PSWN | Public Safety Wireless Network |
| RF | Radio Frequency |
| UHF | Ultra High Frequency |
| VHF | Very High Frequency |


Remote RF Site #2
Auxiliary Operations Center
Dispatcher
Patching
Console
Prime Site
Controller
Remote
Controller
ECC
Communications
Equipment
Dispatch
Consoles
Modem
Message
Switch
Network Management
System
System
Monitoring
Console
Primary RF Site
Remote
Controller
Prime Site
Controller
Back-up
Prime Site
Controller
Remote RF Site #3
Remote
Controller
Remote RF Site #1
Remote
Controller
Data Storage Sites
Data Storage Sites Include:
- Motor Vehicle Department
- National Crime Information Center (NCIC)
- State Crime Information Center
- Local Records Information Center
Each RF Site contains:
- 15 trunked repeaters, 3 are equipped for secure communications
- Repeaters for the primary channel simulcasts
- Uninterruptible power supplies
- Generator backup power
- Entry, heat, and smoke alarms
ECC and Remote RF Site #2 also contain:
- Repeaters for MDT communications

**DRAFT—Do Not Quote or Cite**

Public Safety Wireless Network

# *Security Field Data Collection and Analysis Report*

# *Site #2*
# *Digital Trunked Radio System*

**Final**

July 1999

# FOREWORD

This report presented by the Public Safety Wireless Network (PSWN) program documents security issues and candidate recommendations identified during the second of a series of security field data collection and analysis efforts. The primary goals of these efforts and the resulting reports are to raise security awareness and understanding and to help mitigate security risks associated with evolving public safety communications systems.

Questions or comments regarding the information contained in this document should be forwarded to the PSWN Program Management Office (PMO) at 800-565-PSWN. For additional information regarding the purpose and goals of the PSWN program, see the PSWN web site at www.pswn.gov.

# TABLE OF CONTENTS

**Page**

**1. INTRODUCTION ..... 1**

1.1 PURPOSE ..... 1
1.2 SCOPE ..... 2
1.3 DOCUMENT ORGANIZATION ..... 2

**2. APPROACH ..... 4**

**3. SYSTEM DESCRIPTION ..... 5**

3.1 GENERAL ..... 5
3.2 SYSTEM CONNECTIVITY AND MANAGEMENT ..... 5
3.3 DISPATCH CENTERS ..... 7
3.4 ENCRYPTION CAPABILITIES ..... 7
3.5 PHYSICAL ACCESS TO SYSTEM COMPONENTS ..... 8

**SYSTEM SECURITY FINDINGS ..... 9**

4.1 SECURITY ISSUES ..... 9
*4.1.1 Physical Security at the NCC and a Dispatch Center Is Relatively Weak ..... 9*
*4.1.2 Dial-in Modems at the Primary Site Could Be Exploited ..... 11*
*4.1.3 No Comprehensive Contingency or Disaster Recovery Plan Exists ..... 12*
*4.1.4 No Consolidated Security Policy or Procedures Exist ..... 14*
*4.1.5 Communications System Data Maintained on the Agency's Local Area Network Is Not Adequately Controlled ..... 14*
4.2 BEST SECURITY PRACTICES ..... 15
*4.2.1 System Has Strict Configuration Management ..... 15*
*4.2.2 Data Is Backed Up Regularly ..... 15*
*4.2.3 Alarm and Control Monitoring Occurs at Antennae Sites ..... 16*
*4.2.4 Adequate Environmental Controls Are in Place ..... 16*
*4.2.5 Self-Contained Maintenance Capability Exists ..... 16*
*4.2.6 Communications Are Not Readily Available to Unauthorized Personnel ..... 17*

**5. SUMMARY ..... 18**

APPENDIX A—ACRONYMS ..... A-1
APPENDIX B—SECURITY FIELD DATA COLLECTION PLAN ..... B-1

**1.**

# 1. INTRODUCTION

The Public Safety Wireless Network (PSWN) program has deployed case study teams to conduct detailed interviews with managers and users of public safety radio systems in selected regions of the United States. The case study interview guides used by these teams include several security-related questions. The PSWN program also has initiated a number of security-focused data collection and analysis activities. These data collection activities build on the security information gathered through the case studies by collecting more detailed security information at a few selected sites. A *Security Field Data Collection Summary Report* will be prepared at the conclusion of the initial series of security-focused data collection efforts. These efforts support the larger goal of establishing the PSWN program as a valuable information resource and a source of guidance for many aspects of public safety communications.

Under the security data collection and analysis effort, a first site visit was conducted at an Emergency Communications Center serving police, fire, and emergency medical services on October 8, 1997. The first site is the control center for an analog trunked system. The results of the first site visit are documented in the *Security Field Data Collection and Analysis Report Site #1 – Analog Trunked Radio System*.

A second site visit was conducted from November 9 through 13, 1998, at a Network Control Center (NCC) for a digital trunked radio system serving state and local public safety agencies. In addition to the NCC, a zone controller site, a remote radio site, and a dispatch center were visited in the course of gathering data about the system. This report documents the results of those efforts. All references to the agency visited have been removed from the report.

When conducting a site visit, the PSWN team uses an internally prepared security data collection plan as a guide to ensure all pertinent information is collected. This plan is included as Appendix B of this report. Site visits provide the PSWN team an opportunity to improve the plan based on lessons learned following each visit. This process ensures the PSWN team requests the latest, most accurate, security relevant information at subsequent site visits.

## 1.1 Purpose

The security field data collection activities will increase understanding of the emerging security issues associated with evolving public safety communications infrastructures. These efforts will provide insight into not only the risks associated with the computerization and digitization of those infrastructures, but also the security concerns and needs of the public safety community. In addition, the studies will identify best security practices and measures taken to decrease the risk to public safety radio components and information.

Security field data collection activities support the following goals:

- Identifying the criticality and sensitivity levels of data communicated
- Documenting communications infrastructures used, including wireless and wireline connectivities
- Describing existing technical and procedural security controls
- Identifying security concerns, as well as the frequency and nature of known security issues and incidents
- Capturing existing best security practices and security measures.

Additional security issues, concerns, and practices will be documented as data are collected at additional public safety agency sites. Those findings, along with the findings in this report, may reveal patterns or commonalities in the security of public safety communications. Dissemination of security issues, best practices, and candidate recommendations to the public safety community should provide valuable guidance as the community makes decisions about the security of its systems.

## 1.2 Scope

The security-focused field data collection is intended to gather security-related data on public safety communications infrastructures to enhance the understanding of possible risks to these infrastructures. This report is not an evaluation of the security practices of any particular public safety agency or of public safety communications infrastructures in general. Candidate recommendations are included for each security issue identified in the report. These recommendations and new candidate recommendations will continue to be evaluated during subsequent data collection activities for potential inclusion in a summary report.

## 1.3 Document Organization

This document is divided into the following sections:

- Section 1, Introduction—presents background, purpose, scope, and document layout.
- Section 2, Approach—describes the approach used in conducting the security field data collection and analysis.
- Section 3, System Description—presents a description of the system analyzed and the organization visited.
- Section 4, System Security Findings—presents issues identified during the data collection effort and any best practices used by the subject organization to secure its system.
- Section 5, Summary—provides a synopsis of the findings discussed in the previous section.

- Appendix A, Acronyms—contains a list of acronyms used in this report.
- Appendix B, Security Field Data Collection Plan—includes the data collection approach and detailed interview guide questions used during the site interviews.

## 2.

# APPROACH

A four-step process was used to perform this security field data collection effort. The steps for this approach are described below.

**Step 1: Coordinate and prepare for data collection effort**

- Send the data collection plan for pre-data collection
- Identify personnel for conducting the security data collection effort
- Coordinate the data collection schedule
- Determine which site personnel should be interviewed
- Identify the type of system components at the site for pre-interview research.

**Step 2: Collect system and site data**

- Validate system information collected in Step 1
- Collect more detailed information about the site's system configuration, including a system diagram if possible
- Identify current security practices, concerns, and needs.

**Step 3: Research and clarify data gathered from the site**

- Collect data from various sources (e.g., Internet, professional journals) concerning security issues and concerns raised
- Recontact site personnel, if necessary, to clarify information gathered.

**Step 4: Analyze and document security issues, candidate recommendations, and best practices**

- Describe the security issues raised during data collection
- Provide candidate countermeasure recommendations, as applicable, for security issues
- Document existing best practices at the site
- Consolidate the site data and their analysis into a report.

**3.**

# SYSTEM DESCRIPTION

The NCC visited under this effort is responsible for the management and control of a digital trunked radio system that is serving state and local public safety agencies. Figure 1 provides an overview of the system and its connectivity. The following subsections describe various aspects of the system.

## 3.1 General

The statewide implementation of the communications system includes construction of new communication towers around the state. Currently, the communications system is operating in Phase 1 of four phases, which covers approximately one-fifth of the state's geographic area. The communications system supports 1,000 trunked channels and 134 frequency pairs for local, district, and statewide communications. At present, the system supports only voice communications; however, if a cost effective trunked data solution becomes available in later versions of the current protocol, the agency will consider using it to transmit data on the system.

The state agency that owns the system has sole and exclusive responsibility for the selection of equipment, operation, management, and maintenance of the system and its services. The state agency staffs the NCC 24 hours a day, 7 days a week to assist user agencies and to support troubleshooting of the communications system.

## 3.2 System Connectivity and Management

The communications system has integrated communications controllers at the site, zone, and wide area levels. The NCC is connected to the trunked communications system by digital DS1 circuits. The digital microwave system connects all other sites into a system and uses 6 GHz for high capacity links and 6 GHz and 18 GHz for low capacity links. The microwave radio paths provide reliability of equal or greater than 99.999% and have an outage time less than 5.25 minutes per year. Microwave hops 25 miles or longer uses space diversity protection to eliminate multipath fading. Each path has a fade margin value greater than 40 dB per hop. Elliptical waveguide and tunable connectors are used to connect the microwave radio system to the antennas.

For the trunked communications system, fault tolerance is provided for on both the wide area and local levels. The zone controller that manages the trunked system is equipped with redundant cards, power supplies, and hard drives for all functions. In addition, the system uses alternate paths to maintain wide area coverage when a single point of failure occurs. If an alternate path is unavailable due to multiple points of failure, communications are still locally available using the built-in site trunking mode. If the site trunking mode becomes unusable, then radio to radio communications is available in the "Fail Soft" mode (base stations revert to conventional repeaters) as a last resort.

NCC personnel and agency communications division staff control and manage the system. The on-duty NCC operator uses a network management system and an alarm monitoring system to configure, control, and monitor the radio sites and the communications system. Both the management and alarm systems are connected to the primary radio site via leased lines. In addition, there is dial-in access to the primary site to allow communications division staff and the vendor to configure and control the system remotely when required.

NCC personnel and agency communications division staff develop and maintain talkgroup templates used for programming user radios. The same personnel also control the system key required to program radios, ensuring that only approved changes are made to radio unit templates. Each radio has a unique electronic identification (ID) that is checked by the system each time a transmission is made to make sure only valid devices use the system. The NCC system can make a lost or stolen radio invalid which prohibits it from transmitting or receiving any communications. If a lost or stolen radio is unreachable (i.e., turned off), the system will continue to attempt to invalidate the radio until successful. Once a lost or stolen radio is recovered, it can again be made valid.

### 3.3 Dispatch Centers

Seven statewide dispatch centers and one local dispatch center per county are planned for the system. Dispatch centers will consist of both computer-aided dispatch (CAD) and non-CAD systems for the immediate future. There are two to ten dispatchers, depending on the location, per shift to operate the dispatch consoles. The dispatch centers have the capability to record any conversation for up to 20 minutes in duration.

### 3.4 Encryption Capabilities

All channels are able to transmit either clear or encrypted voice communications and encryption is provided for those agencies that require it for their communications. All trunked repeaters in the system can relay encrypted voice between units with minimum degradation of audio quality and no decrease in the coverage compared to the quality and coverage for clear voice. Approximately 20 percent of radios, currently available or planned, support encrypted communications. The encryption mechanism used is Federal Information Processing Standard (FIPS) 140-1 compliant and the system is intended to migrate to be compliant with the Telecommunications Industry Association/Electronics Industry Association (TIA/EIA)-102 (Project 25) standards.

### 3.5

### Physical Access to System Components

Physical access to all radio sites is restricted to authorized personnel. Fencing with locked gates is installed around the site perimeters. Entrance doors into the buildings that house communications and support equipment are locked at all times. Uninterruptible power supplies and generator backup power are provided at all radio sites. The site buildings were constructed with solid concrete and fire proof material on the walls and ceilings. Additionally, each site has entry, heat, and smoke alarms that send a notification to NCC personnel.

During normal working hours, a receptionist at the main entrance controls access to the building that houses the NCC. The entrance and exit to the parking lot, the main entrance to the building, and access to the floors within the building are controlled by swipe card devices during nonworking hours. At the time of the site visit, swipe card access was used only at two side entrances and one interior door of the building during normal working hours.

Since there are only 200 people located in the building, the agency determined that there is no need for a physical security officer to be assigned to the building. However, a security officer from the state agency headquarters performs security duties such as issuing swipe cards and keys as needed.

# 4. SYSTEM SECURITY FINDINGS

This section describes the security issues and the best practices identified during the site visit and as a result of subsequent follow on discussions with site personnel.

## 4.1 Security Issues

The security issues described in this section include possible implications or associated risks along with candidate recommendations on mitigating the risks. Table 1 summarizes the identified security issues and the corresponding recommendations. The following subsections provide more details.

**Table 1**
**Summary of Security Issues and Candidate Recommendations**

| Section | Security Issue | Candidate Recommendation |
|---|---|---|
| 4.1.1 | Physical security at the NCC and a dispatch center is relatively weak. | The main entrance to the building housing the NCC should be swipe card activated at all times. Swipe card controls on the interior stairwell doors should be activated at all times. Lock doors providing access to NCC, or install and activate swipe card readers for those doors. |
| 4.1.2 | Dial-in modems at the primary site could be exploited. | Network managers should be made aware of network dial-in vulnerabilities and security practices (e.g., modem dial-back, token-based authentication, password parameter settings). Security policies should address this remote management and maintenance point of entry. |
| 4.1.3 | No comprehensive contingency or disaster recovery plan exists. | Develop comprehensive contingency/disaster recovery plans that address operational procedures to be followed by dispatchers, radio users, and management. The contingency plans should be tested periodically based on the criticality of operations. |
| 4.1.4 | No consolidated security policy or procedures exist. | Develop agency security policy and procedures applicable to the communications system and make them available to personnel responsible for implementing, operating, and maintaining the communications system. |
| 4.1.5 | Communications system data maintained on the agency's LAN is not adequately controlled. | Restrict access to the communications system data maintained on the agency's LAN to only those personnel that require access to the data to perform their mission. |

### 4.1.1 Physical Security at the NCC and a Dispatch Center Is Relatively Weak

The building that houses the NCC is accessed by entering a fenced and gated parking lot and then entering the building's main entrance door or one of two side entrance doors. Both the entrance and exit gates to the parking lot and all three exterior building entrance doors are swipe card enabled. However, during normal working hours, the parking lot gates are left open and the

main entrance "visitor door" does not require use of a swipe card to enter the building. There is a receptionist at the main entrance to the building during these hours; however, on two occasions during the site visit, the receptionist was not present when the building was entered. The interior stairwell entrances to each floor and the elevator keypad are also swipe card enabled. However, at the time of the site visit, the interior stairwell doors were all keyed to be open during normal business hours. Only one interior door of the building was swipe card activated during normal business hours.

The third floor of the building houses the communications division and other staff of the public safety agency. The NCC is located on this floor and has doors on two hallways. Both hallway doors are not locked and are typically left open. The combination of the third floor and building access controls, or lack thereof, implies that a person with everyday access to the building could easily gain access to the third floor and the NCC. In addition, anyone could gain access to the building and then to the third floor and the NCC with little trouble.

Access to a dispatch center was also poorly controlled. The building that houses the dispatch center is accessed by entering either an "open" parking area outside the fenced compound and then walking inside the compound, or entering a fenced and gated parking lot within the compound and then entering the building. At the parking lot entrance is a guard booth with swipe card reader and a wooden, raisable entrance arm. However, the guard booth was not manned during the site visit and anyone could either walk around the raisable entrance arm or break it by driving through the arm. The building entrance was not locked.

The dispatch center was located one floor above the building entrance. Entrance to the dispatch center itself was controlled by personnel within the dispatch center. Visual recognition or presentation of an appropriate employee badge and visit coordination was required. Further, it was noted that the dispatch center had a video monitor which, on a rotating basis, displayed the parking lot area, the gate entrance, the building entrance door, and a guard station in another building that controlled access through the gate. However, only one desk at the dispatch center had a clear view of the monitor displaying the entrances. It was stated during the site visit that as late as 11:00 p.m. the building entrance was unlocked.

**Candidate Recommendation:**

Ideally, the building housing the NCC should have its main entrance controlled to allow only authorized visitors and personnel into the building. Activating the swipe cards on the parking lot during normal business hours would probably be a significant inconvenience to authorized personnel. It would seem a reasonable compromise to have the main entrance swipe card activated at all times with the receptionist having the capability to allow entrance to the facility, as required. Access within the building and to the NCC should also be controlled. Activating the swipe card controls on the interior doors, assuming that all authorized building tenants would be authorized access to all floors, would ensure that only building occupants could gain access to a floor. In addition, either the NCC should have its doors locked during normal business hours, or swipe card readers should be installed that allow only authorized staff access to the NCC.

The dispatch center building should have swipe card access capability on the exterior door of the building, or if that is not practical, an interior door installed with swipe card access capability that leads to the dispatch center floor. Consideration should also be given to enabling a swipe card capability on the fence gate at the entrance to the interior parking lot instead of the raisable entrance arm.

During a conversation with the public safety agency that occurred after the site visit, it was discovered that the interior doors of the building housing the NCC had recently been swipe card enabled. This has the effect of minimizing the opportunity for an outsider to gain entrance to the building and then immediately have access to all floors within the building. Any outsider would be restricted to the lobby area until escorted or until provided with a badge allowing freedom of movement within the building.

### 4.1.2 Dial-in Modems at the Primary Site Could Be Exploited

The primary site has two dial-in modems that are used for remote administration or monitoring of the radio system. One modem is used to configure the radio system controllers and to perform maintenance and updates of the radio system software. Connection to the system is controlled by user identification (ID) and password with additional passwords needed to access certain parts of the system. The other modem is used to access the alarm and control system that monitors many different facets of the telecommunications backbone and the physical environment of the remote sites. Connection to this system is also controlled by user ID and password. These two modems introduce an avenue into the system that could be used to modify or compromise many aspects of the radio system. The passwords used for allowing or denying access to the system are not currently configured to be difficult for an attacker to determine. In addition, there is no method used to limit who or what can connect to the modems.

By allowing connections and access attempts to anyone with a modem, commonly used automated tools called wardialers could exploit these points of entry. Wardialers are used to identify modems among a range of phone numbers. They may be configured to repeatedly attempt to login to a remote computer once a modem connection is made, using numerous user IDs and a dictionary of possible passwords. It is possible to configure wardialers to respond with passwords constructed in accordance with various configuration parameters. Once an attacker has connected to the radio system, a talkgroup could have its name or membership modified, and the whole system could be shut down or made unusable by a determined attacker. Likewise, the potential exists for the alarm system to have its operation maliciously modified or disabled.

**Candidate Recommendation:**

Awareness of the potential vulnerabilities associated with remote access capabilities should be raised in the public safety community because it is likely that similar configurations exist on other public safety communications networks. Security safeguard options should be considered by network managers to mitigate the risk of such vulnerabilities. Options include modems that disconnect and then dial a pre-configured number, authentication mechanisms that require the user to possess a physical device as well as a password, and configuring the password to be difficult to guess but easy to remember (e.g., j0e4*lite—joe for starlight).

### 4.1.3 No Comprehensive Contingency or Disaster Recovery Plan Exists

The system management staff is aware of the importance of contingency plans and has been working on the development of such plans. However, there are no documented contingency plans. Contingency plans should address detailed step-by-step actions to be taken in emergency situations such as when a dispatch center is unavailable, or users are unable to communicate using the wide area communications system. Without documented contingency/disaster recovery plans, individuals may be unaware of their roles and responsibilities under emergency conditions.

**Candidate Recommendation:**

Develop comprehensive contingency/disaster recovery plans that address operational procedures to be followed in an emergency situation that affects the communications infrastructure (e.g., fire at a site, earthquake, storm, and system failure) by dispatchers, radio users, and management. These plans should be available to dispatch centers and all users with responsibilities identified within the plans. The plans should also address how to resume normal operations after the emergency situation has passed.

The contingency plans should be exercised periodically based on the criticality of operations so there can be reasonable assuredness of a continuity of essential operations in the event of a disaster or emergency. The following table presents the frequency with which certain portions of the contingency plans should be exercised.

| Criticality Level | | Description | Frequency |
|---|---|---|---|
| 1 | Critical | • Can only be done by the radio system.<br>• No alternate processing capability exists. | Quarterly |
| 2 | Essential | • Alternate methods available and would be implemented until the radio system is restored. | Bi-annually |
| 3 | Important | • No radio system is needed.<br>• Other methods are available. | Annually |
| 4 | Non-Critical | • Can be delayed until a damaged system is restored and/or new equipment is purchased. | As needed |

### 4.1.4

**No Consolidated Security Policy or Procedures Exist**

No consolidated set of security policies or procedures applicable to the agency's communications system exists. A security policy should describe how an organization manages and protects a system and information about the system. Security procedures should provide users and managers with specific instructions on how to securely interact with a system. Although a number of high level security policies have been developed as called for in the system's Request for Proposal, there is no single document or repository for security information about the system. This makes it difficult for the agency to determine the overall system security posture and for the agency personnel responsible for security to identify how security should be managed.

In addition, the lack of a security policy can lead to an unsecurely configured system and to users not following good security practices. For example, during the site visit it was discovered that users were essentially sharing a user ID and password by leaving a number of systems in the NCC logged in continuously. In effect, shift changes occur with the outgoing user not logging out and the incoming user not logging in but using the system from the time they arrive on shift. In addition, no screen savers are used on the NCC's systems that would require a user to present a password to activate the terminal after a period of inactivity, and users are not required to log out when leaving a system unmonitored for a period of time (e.g., to take a break or coordinate with someone in another office). With the already identified weaknesses in the physical security of the NCC, it would be relatively easy for someone to enter the NCC during such a time and modify system parameters to adversely affect the system.

**Candidate Recommendation:**

Develop agency security policies and procedures applicable to the communications system and make them available to personnel responsible for implementing, operating, and maintaining the communications system. The security policy should enforce security requirements set forth in federal radio communications regulations and directives (e.g., user ID and password should not be shared, passwords should be not easily guessable).

### 4.1.5 Communications System Data Maintained on the Agency's Local Area Network Is Not Adequately Controlled

The public safety agency maintains information about its communications system on the agency's local area network (LAN). This information includes template files, job tickets, network databases, and system drawings. The information is used to assemble billing information for users of the system, to prepare statistical data about the system, and to provide an easy method of retrieving data about the system for management and administrative use. Currently anyone in the communications division is able to access and modify the communications information on the LAN. Billing personnel have only read access to the data.

Although the system data on the LAN is not used to control the communications system, access to it should be controlled. The information on the LAN provides a great deal of critical

information concerning the communications system and its operation that could be useful to someone interested in disabling or manipulating the system. Only communications division personnel that require access to the communications system data in performance of their duties should be allowed access to it.

**Candidate Recommendation:**

Restrict access to the communications system data maintained on the agency's LAN to only those personnel within the communications division that require access to the data to perform their mission. The access control mechanism on the LAN could be used to limit the rights that users or groups of users have to the communications system data. For example, some users could be granted read access while others are granted read and write access based on their operational duties.

## 4.2 Best Security Practices

The "best security practices" identified during the site visit and presented in this section include concepts, designs, and procedures that appear to be reasonable methods of mitigating security risks to public safety communications infrastructures.

### 4.2.1 System Has Strict Configuration Management

Originally the vendor preprogrammed all talkgroups into all radios; however, this process allowed any entity with the appropriate software to activate any talkgroup in their radio even though they were not included within the talkgroup's functional or operational chain. In addition, the same software allows certain features to be activated that could cause unwanted effects on the system. Therefore, the communications division reprogrammed all the radios to contain only the talkgroups needed by the organization owning the radio. In addition, the communications division has maintained rigid control of the system's "control key" that allows certain features and functions to be activated, including adding talkgroups to a radio.

By actively controlling talkgroups programmed into the radios and restricting the features and functions that organizations can activate, the communications division ensures safe and efficient operation of the system. All changes made to radio talkgroup templates or the network database are documented by the requestor, reviewed by the engineering group, and must be approved by communications division management before implementation. User organizations are made aware of the strict configuration management control exercised by the system owner via a user agreement that the system owner and user organization must sign prior to the user organization being included in the system.

### 4.2.2 Data Is Backed Up Regularly

At the NCC, systems that are integral to controlling and monitoring the communications system are backed up weekly or more frequently if there is greater activity in the databases and information that is used by the systems. In addition, information stored on the LAN concerning the communications system is backed up daily as part of the LAN backup process. This

information includes template files, job tickets, network databases, and system drawings. The backup media are stored at off-site facilities after the data is backed up. This practice allows the NCC to restore data in a timely manner if it is lost due to system malfunction.

### 4.2.3 Alarm and Control Monitoring Occurs at Antennae Sites

The communications system has alarm and control monitoring for the trunking equipment, telecommunications backbone equipment, the equipment shelters, and antennae towers. The antennae site perimeters are surrounded by barbed-wire fences and locked gates to dissuade unauthorized persons from gaining access. Only limited personnel have keys for the locked gates. Access to the shelters activates an alarm that is broadcast to multiple locations (primary location being the NCC) where action is taken to validate the alarm, including sending personnel to investigate if the reason for the alarm is undeterminable. The information recorded by the system includes site identity, time of the event, and any other pertinent data concerning the event.

### 4.2.4 Adequate Environmental Controls Are in Place

The antennae sites have adequate environmental controls installed and operational. These controls are:

- Fire extinguishers at each exit door
- Heat and smoke detectors
- Uninterruptible power supplies
- Emergency power provided by auxiliary generators with fuel to operate for extended periods
- Fuel tanks provided with low fuel indicators tied into the alarm system
- Emergency switch and emergency shutdown procedures
- Grounding to protect the sites against lightning hits.

### 4.2.5 Self-Contained Maintenance Capability Exists

The agency operates its own maintenance facility, which provides limited component repair and programs the features, functions, and talkgroup templates into radios. Talkgroup template construction, including feature configuration, is performed by Communications Division staff associated with the NCC.

The agency has exclusive responsibility for operation, management, and maintenance of the radio equipment, including features and functions. The NCC personnel handle requests for radio repair by coordinating transportation of the radios to the maintenance facility. Non-state and other agency mobile radios are maintained by commercial companies. Those companies can do limited component repair and are not permitted to reprogram radio functions or features. Only the agency's radio technicians are able to reprogram the radios and then only with the consent of the NCC personnel and a valid job ticket authorizing the reprogramming. In addition, if a radio

must be shipped to the manufacturer for repair, the internal programming is deleted before shipment, ensuring programming control and system information is maintained by the system owner.

### 4.2.6 Communications Are Not Readily Available to Unauthorized Personnel

Conventional analog communications have long been able to be monitored by the public through the use of radio scanners. Over the past few years, a new generation of trunking scanners has enabled the public to easily monitor trunked analog communications. Both trunked and conventional digital communications may be monitored; however, with current scanning capabilities, the information that is monitored sounds like a series of noises to the human ear. The information is understandable only after another radio within the communications system has "undigitized" the information.

The agency has had requests from outside commercial agencies (e.g., towing companies) to be included in their network so they can monitor transmissions. The agency neither has included these agencies in their network nor has any intention of doing so in the future. The agency also indicated that they had heard of commercial scanner manufacturers requesting digital translation information from radio system manufacturers with the likely intent to produce a scanner capable of monitoring, in an understandable manner, digital trunked radio communications. Additional steps taken by this agency are keeping the control key used for programming radios under their direct control and not allowing wildcard IDs to affiliate with the communications system. Even with these types of precautions, the agency should be aware that it is only a matter of time until a scanner is developed that will allow the public to easily monitor and understand trunked digital radio communications. At that point, only the use of encryption will ensure a high degree of voice communications confidentiality.

## 5.

# SUMMARY

The security issues identified during the second site visit and through subsequent information gathering are documented in Section 4 and are summarized as follows:

- Physical security at the NCC and a dispatch center is relatively weak
- Dial-in modems at the primary site could be exploited
- No comprehensive contingency or disaster recovery plan exists
- No consolidated security policy or procedures exist
- Communications system data maintained on the agency's LAN is not adequately controlled.

The security issues identified are related to physical, communications, and administrative and management security. Controlling access to the facility or dispatch center is one way to easily provide a first level of protection to the system management components. Dial-in access to the system, which is not under the control of the owning agency, increases the risk of unauthorized personnel accessing the system and should not be allowed. Developing and exercising plans, procedures, and policies that specify security processes and provide detailed guidance to agency staff will reinforce the need for security to agency staff and help identify areas in which security can be improved. Limiting access to information about the communications system to the minimum amount of people limits the opportunity for both inadvertent and intentional disclosure of such information.

# APPENDIX A

# ACRONYMS

| | |
|---|---|
| APCO | Association of Public Safety Communications Officials |
| CAD | Computer-Aided Dispatch |
| FIPS | Federal Information Processing Standard |
| ID | Identification |
| LAN | Local Area Network |
| MHz | Megahertz |
| NCC | Network Control Center |
| PMO | Program Management Office |
| PSWN | Public Safety Wireless Network |
| TIA/EIA | Telecommunications Industry Association/Electronics Industry Association |

# APPENDIX B

# SECURITY FIELD DATA COLLECTION PLAN

# DRAFT—Do Not Quote or Cite

# Security Field Data Collection Plan

## 1.0 INTRODUCTION

A series of security field data collection and analysis efforts is being conducted with the primary goals of identifying security issues and concerns associated with evolving digital land mobile radio (DLMR) systems. This *Security Field Data Collection Plan* was developed to ensure consistency and adequate coverage across the organizations at which data is being collected.

## 2.0 APPROACH

The following steps outline the high level approach used in conducting each security field data collection and analysis effort.

### Step 1: Coordinate and prepare for the data collection effort

- Identify personnel for conducting the security data collection effort
- Coordinate the data collection schedule with the organization
- Determine which organization personnel should be interviewed
- Identify the type of system components at the organization for pre-interview research
- Ask for documentation containing descriptions of the identified system components and system diagrams
- Provide the organization point of contact with the Security Field Data Collection Plan security questions and background information.

### Step 2: Collect system and organization data

- Collect data by reviewing the documents and diagrams provided by the organization
- Visit the organization and interview personnel using the data collection plan interview guide
- Validate the collected data
- Tour facility and observe operating environment

- Collect additional system and security information
- Identify current security practices, concerns, and needs.

**Step 3: Research and clarify data gathered from the organization**

- Conduct research on security issues and concerns raised
- Recontact the organization, if necessary, to clarify information gathered.

**Step 4: Analyze and document security issues, candidate recommendations, and best practices**

- Describe the security issues raised during data collection
- Provide candidate countermeasure recommendations for security issues
- Document existing best practices at the organization
- Consolidate the organization data, analysis, and recommendations into a report.

## 3.0 SECURITY QUESTIONS

The security questions found on the following pages are categorized as follows:

- General
- Administrative security
- Physical security
- Automated information system (AIS) and network security
- Communications security
- Portable/mobile radios
- Portable/mobile data
- Other.

These questions serve as guidelines to the interviewer. It is expected that discussions will expand upon these questions. A glossary is provided at the end of this plan to help clarify terms used in the questions.

| **GENERAL** |
|---|
| Agency/Organization:<br>Agency Contact:<br>Job Title/Function:<br>Telephone Number/Fax Number: |
| System operations:<br>• Number of users/radios<br>• Coverage (county, state)<br>• Types of users (police, fire, EMS, other)<br>• Number of dispatch centers/dispatch positions at each center<br>• Number of dispatchers per shift<br>• Number of channels and frequencies |
| Type of equipment used:<br><br>Manufacturer of radio system<br><br>Product name<br><br>Type of services:<br>• Encryption<br>• Voice and data capability<br>• Agencies using mobile data<br>• Paging capability |
| Sensitivity of voice/data stored, processed, or transmitted? (Confidentiality, Integrity requirements)<br><br>Mission criticality of operations? (Availability requirements) |
| May we obtain a high-level system diagram, even if hand drawn? |

| ADMINISTRATIVE MANAGEMENT |
|---|
| **Security Policy** |
| Does a written security plan exist for the RF network and any wireline networks or systems?<br><br>What kind of information does the security plan contain?<br><br>Who is responsible for reading and maintaining the security plan?<br><br>Does a written security policy exist for the organization?<br><br>If yes, does this policy cover AIS and radio systems?<br><br>If yes, is the policy consistently enforced?<br><br>If yes, may we obtain a copy of the written policy?<br><br>HHas any type of security evaluation or security testing been performed at the organization?<br>If yes, when was the last time an ST&E was conducted?<br><br>May we obtain a copy of the ST&E report? |
| **Contingency Plans** |

| ADMINISTRATIVE MANAGEMENT |
|---|
| Is there a contingency plan?<br><br>If yes, what is the scope of the contingency plan?<br><br>Is the contingency plan tested periodically and updated?<br><br>When was the last time the contingency plan was tested and updated?<br><br>Is there any redundancy available for consoles and communications connectivity?<br><br>Is the system capable of operating in a degraded state, if necessary? Please describe.<br><br>Is there a "ready-to-use" site designated in case of unavailability of the primary site?<br><br>Where is the "ready-to-use" site located?<br><br>Do contingency operations (i.e., emergency sites and equipment) provide the same level of security controls as regular operations? |
| **Data Backup** |
| Are the system/network data and resources backed up periodically?<br>• How often are they backed up? (Incremental backup/full backup)<br>• Is there an off-site storage facility for backup media?<br>• How often are the backup media sent to the off-site facility? |
| **Configuration Management** |
| Is there configuration management of computer programs?<br><br>Who is responsible for reviewing and approving any changes made?<br><br>Are all changes made to the system documented? |
| **Security Training** |

| ADMINISTRATIVE MANAGEMENT |
| --- |
| Are users provided security training?<br><br>How often do they receive security training?<br><br>What subjects does the security training cover?<br><br>What methods are used to provide security training (e.g., sessions, memorandums)? |

| ADMINISTRATIVE MANAGMENT |
|---|
| **Personnel Security** |
| Is a personnel security policy established?<br><br>Is a background check required for users (e.g., employees, contractors) prior to gaining access to the system?<br><br>Is a background check required for cleaning and maintenance personnel prior to being hired?<br><br>Is there any additional or more detailed check required for administrators of the system?<br><br>Are contractors and support personnel (e.g., cleaning, vending, maintenance personnel) subject to the same check as users and/or administrators? |
| **Maintenance/Services** |
| Does the organization own the maintenance facilities?<br><br>Who performs equipment maintenance services?<br><br>What type of maintenance services are performed?<br><br>Are maintenance activities monitored to ensure security?<br><br>Is DLMR equipment transported to and from maintenance locations in a secure manner?<br><br>Is equipment tested after being serviced to ensure that security controls or functions have not been tampered with?<br><br>Are all maintenance activities recorded?<br><br>Is the maintenance record kept for a specified period of time? |

| PHYSICAL |
| --- |
| **Facility** |
| Is a physical security officer designated in writing?<br><br>How are the facility perimeters protected?<br><br>Who has access to the communications system *facilities during duty hours?*<br><br>How is access to facilities controlled during duty hours?<br><br>Is there access control at the facility entry (guards/locks)?<br><br>Who has the building master keys for the facilities?<br><br>Are visitors logged in and out?<br><br>Are bags searched upon entry (even if random)?<br><br>Are bags searched upon exit (even if random)?<br><br>Are identification badges required for access?<br><br>Are visitors required to wear badges at all times?<br><br>Are visitors escorted at all times?<br><br>Is surveillance equipment used?<br><br>How is access to facilities controlled after duty hours?<br><br>Who has access to the facilities after duty hours? |
| **Computer Room(s)** |

| PHYSICAL |
| --- |
| What computer room(s) exist to manage and support the organization's communications?<br>• What are the functions of each?<br>• Where are they located?<br>• What type of computer equipment does each computer room house?<br>Who has access to the computer rooms?<br>How are the areas secured where computer equipment is stored?<br>Are doors locked at all times?<br>Are cipher locks used? If so, where/under what conditions?<br>If cipher locks are used, are the combinations changed regularly? When?<br>Are visitors logged in and out?<br>Are visitors escorted at all times?<br>Are computer rooms manned 24 hours a day, 7 days a week? |
| **Dispatch Center** |

| PHYSICAL |
| --- |
| Who has access to the dispatch center?<br><br>What physical security measures (e.g., *guards*, keys, access cards) are used to prevent unauthorized access to the dispatch center?<br><br>Are doors locked at all times?<br><br>Are cipher locks used? If so, where/under what conditions?<br><br>If cipher locks are used, are the combinations changed regularly? When?<br><br>Are visitors logged in and out?<br><br>Are visitors escorted at all times?<br><br>Is surveillance equipment used? |
| **Radio Sites** |

| PHYSICAL |
| --- |
| Who has access to the radio sites?<br><br>Are physical access control measures used to prevent unauthorized access to the sites' perimeters and shelters ?<br><br>Are the radio sites collocated with other agencies, contractors, or commercial organizations?<br><br>If yes, what are the physical security measures used to control the shared sites?<br><br>Do the sites comply with any physical security requirements set forth in the specified regulations (e.g., county jurisdiction code)?<br><br>Do physical access control devices activate alarms at a central location or local police department?<br><br>Are sites regularly inspected by authorized personnel?<br><br>Are the site locations published?<br><br>Are the heat and humidity alarms installed? |
| **Telephone Closet** |
| Who has access to the telephone closet?<br><br>Are doors locked at all times?<br><br>Are keys changed regularly? When? |
| **Environmental** |

**PHYSICAL**

What environmental controls are in place to protect the system and the facility under emergency conditions?

- Are heat and smoke detectors installed in the ceilings and under raised floors?
- Is there a fire alarm?
- Is there a fire suppression system?
- Is the fire suppression system tested periodically?
- Is there a raised floor?
- Are there uninterruptible power supplies?
- Is there an emergency power capability?
- Is there a procedure to ensure that fuel running the auxiliary generators is sufficient and not contaminated?
- Is there an emergency switch and emergency shutdown procedures?
- Is the air conditioning system dedicated to the dispatch center or to the computer room?
- Is backup air conditioning available?
- Is proper grounding provided?
- Are the radio sites properly installed to protect against lightning?
- Is alternate routing available for power and phone services?

**AIS/NETWORK (System/Network Administrators)**

***** Note *****

**This section addresses the questions for system/network administrators responsible for managing any wireline system or network that interfaces with the RF network.**

**Identification and Authentication**

Are there procedures established to manage authorized user accounts on the system/network (e.g., create, delete, disable)?

How are user accounts/passwords distributed?

Identify any password constraints used by your system:

- Password length
- Password composition
- Password aging (How often must passwords be changed?)
- Password history (Are old passwords prohibited from reuse for a certain time period?)
- Change of initial password
- Resetting of forgotten passwords (Is a change then required?)
- User account locked out after a specified number of unsuccessful login attempts.

Are there procedures for handling accounts for users no longer requiring access to the system or network?

Is a list of user accounts maintained, reviewed, and updated? How often?

**Access Control**

Are there different levels of access to the system/network (e.g., users, system/network administrator, security administrator)?

What kind of privileges does each level have?

How are user's access privileges to the system or its data determined?

Is there network-based remote access to the local area network (e.g., Internet, Intranet, WAN)?

| AIS/NETWORK (System/Network Administrators) |
|---|
| **Audit** |
| Are audit trails available? (electronic logs of security related events performed by system users)<br><br>What kinds of security events are recorded in the audit trails?<br><br>Who reviews the audit trails? How often?<br><br>Are security activities on network hosts recorded? If so, who reviews? How often? |
| **Remote Dial-in Access** |
| Is there any dial-in access to the network? If so,<br><br>• Who has dial-in access to the system/network?<br><br>• To what components is dial-in access allowed?<br><br>• What functions are performed remotely?<br><br>• Are there any security controls for the remote access? (e.g., dial-back modem, strong authentication)<br><br>• Are there constraints for failed access attempts?<br><br>– How many times is failed access allowed?<br><br>– What occurs if the number of failed accesses is exceeded?<br><br>Is a list of user accounts for dial-in access maintained, reviewed, and updated? How often? |
| **Other** |
| Is any virus protection provided for the components that are a part of the system/network? |

| AIS/NETWORK (System Users) |
| --- |
| ***** Note *****<br><br>**This section addresses the questions for system users that access the system/network to perform their functions.** |
| **Identification and Authentication** |

| AIS/NETWORK (System Users) |
|---|
| Are you required to present your ID and password before you access the system/network?<br><br>Who assigns your ID and initial password?<br><br>Do you change your initial password at the first login?<br><br>How often do you change your password?<br><br>Are there policies or procedures for selecting passwords?<br><br>What is the minimum length of a password?<br><br>Are you required to select a combination of alphabetic and numeric characters for your password?<br><br>Does the system/network notify you of the need to change your password?<br><br>Are there procedures for reporting forgotten passwords?<br><br>If you forgot your password, who do you contact to receive your password?<br>• Is your password the same password you used or do you receive a default password?<br>• If you receive a default password, do you need to change the password immediately?<br><br>Are there procedures for reporting security incidents?<br><br>Do you know how many attempts you are allowed to enter your user ID or password before your account is disabled?<br><br>Are there procedures for reporting that your account is disabled? |
| **Access Control** |

| AIS/NETWORK (System Users) |
|---|
| What are your responsibilities for controlling access to information on the system?<br><br>Are you restricted to accessing only applications necessary for your job functions?<br><br>If not, what other applications are you able to access?<br><br>Is your terminal disconnected after an extended period of inactivity?<br><br>Do you log out when you leave your terminal unattended? |
| **Remote Dial-in Access** |
| Do you have dial-in access to the system?<br><br>What functions do you perform remotely?<br><br>Are you required to use your ID and password for dial-in access?<br><br>Who assigns your ID and password for dial-in access?<br><br>How often do you change your password ? |
| **Other** |
| Do you run anti-virus software regularly?<br><br>What would you do if you identified a virus on your system? |

| COMMUNICATIONS |
|---|
| **Encryption** |
| Is encryption provided to protect data transported among the system components?<br><br>What type of encryption is used?<br><br>Is encryption method documented and approved?<br><br>Is the control channel encrypted?<br><br>If no, do you have concerns about an unencrypted control channel being used to exploit radio communications?<br><br>In an emergency situation, how is sensitive information transmitted (via a clear channel or an encrypted channel)? |
| **Key Management** |
| Are written guidelines established for the handling and safeguarding of keying materials?<br><br>What is the key lifetime?<br><br>How are encryption keys changed?<br><br>How are key loaders protected?<br><br>How are radios with the current key loaded protected?<br><br>Are there procedures for protecting keys during their life cycle (e.g., generation, distribution, storage, destruction)?<br><br>When keys are compromised, are they destroyed in a secure manner? |
| **Redundancy** |
| Is an alternative communications path available in case a primary path fails?<br><br>Is there adequate backup (spare) communications equipment available? |
| **Emission Security** |
| When the system was designed, had emission security been considered?<br><br>Do you have concerns about electronic emissions being compromised and used to exploit the radio system? |

| RADIO (Portable/Mobile) |
| --- |
| **User Verification** |
| Does the radio authenticate the currently assigned user?<br><br>Do the radio system components authenticate themselves to one another to ensure that only valid radios may be used?<br><br>What are the procedures for managing system users?<br><br>What are the procedures for managing talkgroups or channel assignments?<br><br>• Who assigns users to talkgroups?<br><br>• How are talkgroups assigned? by function?<br><br>• How are channels assigned? (by function?) |
| **Encryption** |

Is encryption provided for radio equipment?

What percentage of mobiles and portables have data?

What type of encryption is used?

Is the encryption on the radio system transparent (e.g., uses end-to-end encryption)?

Are there policies and procedures to enforce the use of the encryption feature?

Do you use the encryption feature?

Do you turn this feature on and off?

Have you experienced any impact on operations due to the use of encryption (e.g., minimized range, degraded voice quality)?

Are multi-encryption modes implemented to meet an interoperable need?

Have you experienced any interoperability problems due to the use of incompatible encryption schemes between your system and others?

Have the cryptographic components used in the system been FIPS 140-1 certified?

If you don't use encryption, what are the reasons that you don't use it?

**Over-the-Air-Rekeying**

Do you currently use over-the-air-rekeying (OTAR)?

- If yes, how is OTAR managed?

- How many people are authorized to manage rekeying?

**Remote Dial-in Access**

Who has dial-in access?

To what components is dial-in access allowed?

What functions are performed remotely?

Are there any security controls for the remote access? (e.g., dial-back modem, strong authentication)

Are there constraints for failed access attempts?

How many times is failed access allowed?

What occurs if the number of failed accesses is exceeded?

**Redundancy**

Is any redundancy available for dispatch consoles and RF network connectivity?

**Lost and Stolen Radio**

What are the procedures for handling lost or stolen radios?

How is the loss reported to radio managers?

Is there a capability to disable such radios?

If such radios contain encryption capabilities, is any different action taken upon their loss than that taken for non-encryption capable radios?

Are procedures established for controlling access to MDTs and radios?

What are the procedures for activating radios recovered from being lost or stolen?

Are procedures in place for the secure disposal/destruction of radios?

Are procedures established for use of the emergency activation button?

**Portable/Mobile Data**

**Portable/Mobile Data**

Does your organization utilize data communications?

What type of MDTs, MDCs, laptops, or portable data terminals used?

| Portable/Mobile Data |
| --- |
| **Property Disposal** |
| Are procedures in place for the secure disposal/destruction of MDTs/MDCs?<br><br>Is all organization/operation's specific data removed from the device?<br><br>For an MDT/MDC that is no longer used by the organization, is information that would allow continued access to the organization's system or data deleted from the central controller (e.g., unit number, identity code)? |

| OTHER |
| --- |
| Do you have any concerns about the security of your voice communications? If so, please explain.<br><br>Do you have any concerns about the security of your data communications? If so, please explain.<br><br>Have there been any incidents concerning the confidentiality, availability, or integrity of your voice or data systems? If so, please explain.<br><br>Please provide information on any other issues or concerns that you have concerning voice and data system security. |

# GLOSSARY

**Access Control**

A technique used to define or restrict the rights or capabilities of individuals or application programs to communicate with other individuals or application programs 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 Information System**

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

**Availability**

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

**Communications Security**

Protection measures to protect data that is transferred using communication lines. This includes ensuring that transactions are not invalid, incomplete, or altered.

**Computer Room**

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

**Confidentiality**

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

**Configuration Management**

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

**Contingency Plan**

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

**Emission Security**

Measures to control decipherable electronic signals unintentionally emitted from an information system and communications equipment.

**Encryption**

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

**Identification**

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

**Integrity**

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

**Jamming**

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

**Key**

When used in the context of encryption, a series of numbers which are used by an encryption algorithm to transform plain text data into encrypted (cipher text) data, and vice versa.

**Key Management**

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

**Land Mobile Radio**

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

**Mobile Data Terminal**

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

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

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

**Password**

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

**Security Plan**

A document which depicts a site's plan for securing its system.

**Virus**

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

**Vulnerability**

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

Public Safety Wireless Network

# *Security Field Data Collection and Analysis Report*

# *Site #3 Trunked Radio System*

**FINAL**

August 1999

# FOREWORD

This report presented by the Public Safety Wireless Network (PSWN) program documents security issues and candidate recommendations identified during the third of a series of security field data collection and analysis efforts. The primary goals of these efforts and the resulting reports are to raise security awareness and understanding and to help mitigate security risks associated with evolving public safety communications systems.

Questions or comments regarding the information contained in this document should be forwarded to the PSWN Program Management Office (PMO) at 800-565-PSWN. For additional information regarding the purpose and goals of the PSWN program, see the PSWN web site at www.pswn.gov.

# TABLE OF CONTENTS


**Page**

**1. INTRODUCTION ..... 1**

1.1 PURPOSE ..... 2
1.2 SCOPE ..... 2
1.3 DOCUMENT ORGANIZATION ..... 2

**2. APPROACH ..... 4**

**3. SYSTEM DESCRIPTION ..... 5**

3.1 GENERAL ..... 5
3.2 SYSTEM CONNECTIVITY AND MANAGEMENT ..... 5
3.3 ENCRYPTION CAPABILITY ..... 7
3.4 PHYSICAL ACCESS TO SYSTEM COMPONENTS ..... 8

**4. SYSTEM SECURITY FINDINGS ..... 9**

4.1 SECURITY ISSUES ..... 9
4.1.1 No Consolidated Security Policy or Procedures Exist ..... 10
4.1.2 An Off-Site Storage Facility Has Not Been Designated for Backup Tapes ..... 10
4.1.3 Physical Security at Several Sites Needs Improvement ..... 11
4.1.4 Logical Unit IDs for Radios Are Manually Assigned ..... 12
4.1.5 Dial-in Modems for the Communications System Could Be Exploited ..... 13
4.1.6 Encryption-Capable Radios Are Not Used in Encrypted Mode ..... 14
4.1.7 Encryption Key Is Not Changed Regularly ..... 14
4.1.8 Mobile Data Are Transmitted in Clear Mode ..... 15

4.2 BEST SECURITY PRACTICES ..... 16
4.2.1 Contingency or Disaster Recovery Plan Exists ..... 16
4.2.2 Self-Contained Maintenance Capability Exists ..... 17
4.2.3 The Radio System Has Strict Configuration Management ..... 17
4.2.4 Data Are Backed Up Regularly ..... 17
4.2.5 Adequate Access Controls to the Radio Communications System Exist ..... 17
4.2.6 Router Is Configured to Accept Only Specific IP Addresses ..... 18
4.2.7 Adequate Environmental Controls Are in Place ..... 18

**5. SUMMARY ..... 19**

**APPENDIX A—ACRONYMS ..... A-1**
**APPENDIX B—SECURITY FIELD DATA COLLECTION PLAN ..... B-1**

# 1. INTRODUCTION

The Public Safety Wireless Network (PSWN) program has deployed case study teams to conduct detailed interviews with managers and users of public safety radio systems in selected regions of the United States. The case study interview guides used by these teams include several security-related questions. The PSWN program also has initiated a number of security-focused data collection and analysis activities. These data collection activities build on the security information gathered through the case studies by capturing more detailed security information at a few sites. A *Security Field Data Collection Summary Report* will be prepared at the conclusion of the initial series of security-focused data collection efforts. These efforts support the larger goal of establishing the PSWN program as a valuable information resource and a source of guidance for many aspects of public safety communications.

In October 1997 under the security data collection and analysis effort, a first site visit was conducted at an emergency communications center serving police, fire, and emergency medical services (EMS). The first site is the control center for an analog trunked system. The results of the first site visit are documented in the *Security Field Data Collection and Analysis Report Site #1 – Analog Trunked Radio System.*

A second site visit was conducted in November 1998 at a network control center (NCC) for a digital trunked radio system serving state and local public safety agencies. In addition to the NCC, a zone controller site, a remote radio site, and a dispatch center were visited in the course of gathering data about the system. The results of the second site visit are documented in the *Security Field Data Collection and Analysis Report Site #2 – Digital Trunked Radio System.*

A third site visit was conducted in April 1999 at a communications center (CC) for a trunked radio system serving police, fire, and EMS. In addition to the CC, a maintenance facility, a primary transmit-receive site, a backup site, and a receive-only site were visited in the course of gathering data about the system. This report documents the results of those efforts. The report does not include specific references to the agency that would enable it to be identified.

When conducting a site visit, the PSWN team uses an internally prepared security data collection plan as a guide to ensure all pertinent information is collected. This plan is included as Appendix B of this report. Site visits provide the PSWN team an opportunity to improve the plan based on lessons learned following each visit. This process ensures the PSWN team requests the latest, most accurate, security relevant information at subsequent site visits.

## 1.1 Purpose

The security field data collection activities will increase understanding of the emerging security issues associated with evolving public safety communications infrastructures. These efforts will provide insight into not only the risks associated with the automation of those infrastructures, but also the security concerns and needs of the public safety community. In addition, the studies will identify best security practices and measures taken to decrease the risk to public safety radio components and information.

Security field data collection activities support the following goals:

- Identify the criticality and sensitivity levels of data communicated
- Document communications infrastructures used, including wireless and wireline connectivities
- Describe existing technical and procedural security controls
- Identify security concerns as well as the frequency and nature of known security issues and incidents
- Capture existing best security practices and security measures.

Those findings resulting from analysis of the data collected at the previous public safety agency visits, along with the findings in this report, may reveal patterns or commonalities in the security of public safety communications. Dissemination of security issues, best practices, and candidate recommendations to the public safety community should provide valuable guidance as the community makes decisions about the security of its systems.

## 1.2 Scope

The security-focused field data collection is intended to gather security-related data on public safety communications infrastructures to enhance the understanding of possible risks to these infrastructures. This report is not an evaluation of the security practices of any particular public safety agency or of public safety communications infrastructures in general. Candidate recommendations are included for each security issue identified in the report. These recommendations will be evaluated for potential inclusion in a summary report.

## 1.3 Document Organization

This document is divided into the following sections:

- Section 1, Introduction—presents background, purpose, scope, and document structure.
- Section 2, Approach—describes the approach used in conducting the security field data collection and analysis.

- Section 3, System Description—describes the system analyzed and the organization visited.
- Section 4, System Security Findings—presents issues identified during the data collection effort and any best practices used by the subject organization to secure its system.
- Section 5, Summary—summarizes the findings discussed in the preceding section.
- Appendix A, Acronyms—lists acronyms used in this report.
- Appendix B, Security Field Data Collection Plan—includes the data collection approach and detailed interview guide questions used during the site interviews.

# 2. APPROACH

A four-step process was used to perform this security field data collection effort. The steps for this approach are described below.

**Step 1: Coordinate with the agency's point of contact and prepare for data collection effort**

- Send the agency the data collection plan for pre-data collection
- Identify personnel who will conduct the security data collection effort
- Coordinate the data collection schedule.

**Step 2: Collect system and site data**

- Collect detailed information about the site's system configuration
- Identify current security practices, concerns, and needs.

**Step 3: Research related information and clarify data gathered from the site**

- Collect data from various sources (e.g., Internet, professional journals) concerning security issues and concerns raised
- Recontact site personnel, if necessary, to clarify information gathered.

**Step 4: Analyze and document security issues, candidate recommendations, and best practices**

- Describe the security issues raised during data collection
- Provide candidate countermeasure recommendations, as applicable, for security issues
- Document existing best practices at the site
- Consolidate the site data and their analysis into a report.

# 3. SYSTEM DESCRIPTION

The CC visited under this effort manages and controls a trunked radio system that serves municipal public safety organizations. Figure 1 provides an overview of the system and its connectivity. The following subsections describe various aspects of the system.

## 3.1 General

The trunked land mobile radio system, installed in 1992, has undergone several major upgrades (e.g., introduction of data, adding new channels and consoles). The system handles 160,000 push-to-talks (PTT) per 24-hour period. Sixty percent of the PTTs are voice traffic, and the rest are data. The system provides a user-estimated 98-percent portable in-street coverage of the service area for both voice and data. In-building coverage of the service area is estimated to be somewhat less. In its current configuration, the radio system supports the following:

- Twenty-four radio channels:
  - Twenty 25-kHz (wideband) channels used for both voice and data traffic
  - Four 12.5-kHz (narrowband) channels used exclusively for data traffic
- Digital control channel signaling
- Analog voice channels
- Transmission trunking
- Eight T1 microwave (10 GHz) backbone (seven used and one spare T1 capacity is shared with a separate agency system)
- In-building bi-directional amplifiers in critical buildings.

The radio system supports 6,000 user radios with over 2,000 available and 164 in-use talk group identifications (ID) and 350 installed mobile computer terminals (MCT). During the data collection effort, it handled a significantly increased amount of traffic during a major multijurisdictional emergency.

## 3.2 System Connectivity and Management

The CC serves as the 9-1-1 emergency reporting center for the municipal area and as the dispatch center for police, fire, and EMS units. The center is staffed by approximately 50 trained professional personnel. The CC's main communications are supported by a mobile radio system with a computer-aided dispatch (CAD) system. The system is designed to handle an earlier version of analog voice encryption that reduces audio quality.

The CC is connected to the rest of the communications system by an 10-GHz digital microwave radio system. The microwave radio system provides 99.999 percent reliability. Currently, there is no backup capability for the microwave radio system because having a backup site is not considered cost effective.

Control and management of the radio system are performed by the CC radio system manager. The radio system manager uses a network management system and system-monitoring software to configure, control, and monitor the system. The network management system provides an interface point for the entire radio system. Communications between the network control terminal at the maintenance facility and the network management system are transmitted through the agency's citywide local area network (LAN), which is connected to a router via frame relay. A computer running the network management system and the monitoring software is hardwired to the primary site and runs on a Windows NT 4.0 server. There is dial-in access to the computer to allow the radio system manager or authorized personnel (i.e., system vendors) to control the radio system remotely when required. Dispatchers can perform dispatch-related control of the radio system from the dispatch console. Seventeen operator consoles are located at the CC.

Radio technicians at the maintenance facility develop and maintain talkgroup templates used for programming user radios. The same personnel also control the system key required to program radios, ensuring that only approved changes are made to radio unit templates. Each radio has a logical unique ID that is checked by the system each time a transmission occurs to make sure only valid devices use the system. The system can make a lost or stolen radio invalid over the air.

There are two transmit-receive sites (one primary and one backup) and two voted receive-only sites. If the primary site fails, the system will be manually switched to be operated from the backup site. The backup site is tested once a month. Additionally, the system is designed to be inherently robust by using a fail-soft technology. When the controller fails, the system operates in the fail-soft trunking mode.

Uninterruptible power supplies and generator backup power are provided at all radio frequency (RF) locations and at the CC.

### 3.3 Encryption Capability

The system supports unit-to-unit analog encryption. The type of encryption utilized is of an older design, which significantly reduces the audio quality and coverage range. The poor audio quality of the encrypted signal is noted as one reason users are reluctant to use the system in the encrypted mode. About 300 radios are capable of encryption operation. These radios are typically issued to officers working in special areas, such as the narcotics, car theft, and gang divisions. The key loading device is maintained by the maintenance facility, and the encryption key is stored in a locked drawer. The current system is not capable of over-the-air-rekeying (OTAR) operation.

## 3.4 Physical Access to System Components

Physical access to all radio sites is restricted to authorized personnel. The building where the CC and the backup site reside is fenced in and closed with a locked gate. Access to the CC is controlled by requiring entrance through two cipher lock enabled doors. Receive-only sites, located at leased facilities, are physically secured by a combination of locked doors and controlled access to the spaces they occupy (e.g., on the upper floor of an office building). A physical security officer designated at the CC is responsible for managing and controlling the keypad distribution and reviewing building access logs.

# 4. SYSTEM SECURITY FINDINGS

This section describes the security issues and the best practices identified during the site visit and as a result of follow-on discussions with site personnel.

## 4.1 Security Issues

The security issues described in this section include possible implications or associated risks along with candidate recommendations on mitigating the risks. Table 1 summarizes the identified security issues and the corresponding recommendations. The following subsections provide more details.

**Table 1**
**Summary of Security Issues and Candidate Recommendations**

| Section | Security Issue | Candidate Recommendation |
|---|---|---|
| 4.1.1 | No consolidated security policy or procedures exist. | Develop agency security policy and procedures applicable to the communications system and make them available to personnel responsible for implementing, operating, and maintaining the communications system. |
| 4.1.2 | An off-site storage facility has not been designated for backup tapes. | Designate an off-site storage facility for backup tapes. |
| 4.1.3 | Physical security at several radio sites needs improvement. | Agencies whose radio sites are collocated with other organizations should implement additional physical security mechanisms to restrict access to the areas where their radio equipment is housed. |
| 4.1.4 | Logical unit IDs are manually assigned. | Use a database management system with a unique index field to avoid assigning duplicate unit IDs. |
| 4.1.5 | Dial-in modems for the communications system director could be exploited. | Radio system managers should be made aware of network dial-in vulnerabilities and security practices (e.g., modem dial-back, token-based authentication, password parameter settings). Security policies should address this remote management and maintenance point of entry. |
| 4.1.6 | Encryption-capable radios are not always used in an encryption mode. | Enforce regular use of encrypted radios to enhance user confidence; however, agencies should ensure that security mechanisms will not significantly interfere with operations. Consider using digital voice communications of which, when encrypted, will minimally degrade audio quality and not decrease coverage. |
| 4.1.7 | Encryption key is not changed regularly. | Consider using the OTAR feature that allows radios to be rekeyed or zeroized remotely. Agencies should ensure that all key materials are generated, distributed, stored, and destroyed in a secure and controlled manner. |
| 4.1.8 | MDT data are transmitted in clear mode. | Employ encryption techniques because they may be the only solution for lessening the probability of public safety communications being intercepted by unauthorized personnel. |

### 4.1.1 No Consolidated Security Policy or Procedures Exist

A security policy describes how an organization manages and protects a system and information stored and transmitted on the system. Security procedures provide users and managers with specific instructions on how to securely interact with a system. Currently, no consolidated set of security policies or procedures applicable to the agency's radio communications system exists. Therefore, there is no single document for security information about the system (e.g., security plan). Although agency personnel realize how important it is to secure the radio communications system, without a consolidated security policy, it is difficult for the agency to determine the overall system security posture and for the agency personnel responsible for security to understand how security should be managed.

Without a written security policy, there is no assurance that a system is securely configured; nor can users know they are consistently following good security practices. For example, users with encrypted radios might not use encryption consistently. Although user identifications (ID) and passwords restrict access to the radio system, no stringent passwords constraints might be enforced and used (e.g., regular change of passwords, minimum length of password, password age and history).

**Candidate Recommendation:**

Agency-specific security policy and procedures that are applicable to its land mobile radio system should be developed. The security policy should be made available to personnel responsible for implementing, operating, and maintaining the communications system. The security policy should enforce security requirements set forth in federal radio communications regulations and directives (e.g., voice and data radio transmissions shall be protected from unauthorized interception; passwords shall be changed regularly).

### 4.1.2 An Off-Site Storage Facility Has Not Been Designated for Backup Tapes

Network management and data systems are backed up regularly (i.e., twice a month). However, the backup tapes are currently stored on site in a firebox in the room where the system resides. If a natural disaster made the on-site backup tapes unavailable or unusable, the systems would lose all the data stored on the servers. Thus, it would be very difficult to recover the network management systems; thus, system monitoring and controlling functions would be unavailable.

**Candidate Recommendation:**

Designate an off-site storage facility and send a full set of backup tapes to the facility periodically (e.g., once a month).

### 4.1.3 Physical Security at Several Sites Needs Improvement

Overall, the buildings and rooms housing radio equipment provide limited physical security controls through keys, electronic access devices (i.e. keypads), or fenced perimeters. However, since the agency's radio sites are shared with other organizations, their physical security may need strengthening to restrict access to the rooms housing the agency's radio systems and equipment to authorized agency personnel only.

The building that houses the CC is accessed by entering a fenced and gated parking lot and then two entrances. All vehicles and individuals entering the gate should be verified by CC personnel through an intercom. The parking lot entrance is monitored by CC personnel 24 hours a day, 7 days a week. Access to both building entrance doors and the CC is controlled through keypads and keypad access codes. These keypad access codes are distributed to individuals by a physical security officer. Access to any area with keypads is recorded in a proprietary application. These records are reviewed regularly by the physical security officer. However, concern was expressed regarding the building entrance doors, which can be forced open easily without using the keypad because the door is made of light material. In addition, CC personnel may release their keypad access codes to their family or friends so they can enter the building without being escorted.

The agency's maintenance building is accessed by entering the main entrance door and also two side doors. These three doors are locked and alarmed after duty hours. There is a receptionist at the main entrance to the facility during the work hours; however, no challenge was made to visitors when the building was entered, and no visitors' log sheet was available. The side doors are also left open during the work hours so public safety vehicles can enter for repair. Although police cars parked outside of the building and police officers in the building may dissuade unauthorized personnel from entering the building, anyone could gain access to the building and manipulate the computers and possibly steal radio equipment.

The primary transmit-receive site is collocated with other civil organizations. Access to the shared site is controlled through a barbed-wire fence, a key, closed circuit televisions (CCTV), and an alarmed door. Access to the shared site activates an alarm that is transmitted to the landlord, who then acts to validate the alarm. The agency's radio system is located in a locked room. Although a limited number of personnel have the room key, access to the room is not alarmed or monitored by agency personnel.

A receive-only site is also collocated with other organizations. Access to the site is controlled through receptionists, keys, log sheets, and elevator attendants. The agency's radio equipment is located in a locked room, but there is no alarm or control monitoring device available. During the site visit, it was noted that maintenance sheets are not signed consistently to record information on the work performed on the radio equipment.

**Candidate Recommendation:**

If feasible, the building entrance doors to the CC should be replaced with a metal door or another type of door made of heavy material. Security awareness and training should also be provided to personnel at the CC regarding their responsibilities for protecting their access codes from unauthorized disclosure.

It may not be ideal to lock all the doors of the maintenance building during normal work hours because that would hamper operations within the maintenance building. Originally, the building was surrounded with a fenced perimeter and the gate was safeguarded. Similar physical access controls should be established to restrict access to the perimeter compound and the parking lot. These changes will minimize the opportunity for an outsider to quickly access the building.

The primary transmit-only and receive-only sites should have alarm devices installed at the room doors so that access to the rooms activates an alarm that alerts CC personnel to validate the alarm and take appropriate actions. In addition, visitor log sheets should be placed at the sites, and the maintenance sheets should be signed by maintenance personnel every time they work on equipment.

### 4.1.4 Logical Unit IDs for Radios Are Manually Assigned

Logical unit IDs are assigned to portable and mobile radios for radio-to-radio communications. These unit IDs are assigned manually by using spreadsheets to match with presynchronized cards installed in the radios. However, incidents have occurred where duplicate unit IDs were assigned to several radios. This problem was detected by dispatchers who notified the radio system manager of the problem. Radios with duplicate unit IDs may enable spoofing (i.e., transmit with the appearance of being sent by an authorized user of the radio), resulting in confused radio communications. Additionally, users with the same radio unit IDs cannot be held accountable for their actions, especially in an environment where three users share a radio. The duplicate unit IDs may also result in confusion during an emergency button activation.

**Candidate Recommendations**:

To avoid assigning duplicate unit IDs, a database management system, can be used to provide a unique index field that will not allow duplicate numbers as well as fields for radio cards and unit serial numbers. For example, if a radio is assigned with a unit ID, "unit001," the next sequential number will be "unit002." The agency could also consider using programmed unit IDs for radios to be assigned. These methods will avoid human error in assigning radios with duplicate unit IDs.

### 4.1.5 Dial-in Modems for the Communications System Could Be Exploited

A few agency personnel and contractors have dialup access to the network management system and the wireless data system to configure the radio system remotely and to maintain and update the system software. These modems introduce a possible avenue into the system that could be used to modify or compromise the radio system. Connection to the system is controlled by user ID and password, but the passwords are not currently configured to be difficult for an attacker to determine. For example, passwords have not been set to expire and to require a minimum length (e.g., six characters), no numbers or special characters are used, and they are not changed regularly. In addition, contractors use the same password to access the radio system. Passwords that are not changed or that have a long lifetime are more likely to be compromised, allowing unauthorized users to gain access to the radio system. This could result in unauthorized modification or destruction of critical information.

In addition, the "Guest" account was enabled on the Windows NT-based network management system at the time the data collection team made its site visit. This account was enabled as a part of the installation procedure for the network management system, which was taking place during the same timeframe as the site visit. This account was disabled shortly after the site visit took place, with the completion of the network management system's installation.

While the "Guest" account was active, the potential for certain security events increased. For example, unauthorized user could have accessed the system without user ID and password. Commonly used automated tools called "wardialers" could exploit these points of entry. Wardialers are used to identify modems among a range of phone numbers. They may be configured to repeatedly attempt to log in to a remote computer when a modem connection is made, using numerous user IDs and a dictionary of possible passwords. It is possible to configure wardialers to respond with passwords constructed in accordance with various configuration parameters. When an attacker has connected to the radio system, a talkgroup could have its name or membership modified; and the whole system could be shut down or otherwise made unusable by a determined attacker.

The system offers a "lock-out" feature that can restrict unauthorized access to the radio system. However, the system is not set to lock out user accounts after several unsuccessful login attempts. Although the radio system provides audit trails that are reviewed regularly, an unsecured configuration can be exploited by attackers using commercially available penetration tools.

**Candidate Recommendation:**

Windows NT-based applications are in use within the public safety community that are in compliance with Year 2000 (Y2K) requirements. Radio system managers should be familiar with security features provided by the system and configure them securely. The Windows NT operating system provides various security features that can be configured; however, if these

features are not configured securely, they introduce additional vulnerabilities into the system. Therefore, security safeguard options should be considered by radio system managers to mitigate the risk of such vulnerabilities (e.g., modem dial-back, token-based authentication, password configuration constraints). Awareness of the potential vulnerabilities associated with various network access methods should be raised in the public safety community because it is likely that similar remote access "conveniences" exist on other public safety communications networks.

### 4.1.6 Encryption-Capable Radios Are Not Used in Encrypted Mode

Currently, users having radios with encryption capability do not use that capability consistently because of poor voice quality when operating in the encrypted mode. Users not regularly using the encryption capability complain of the voice quality, whereas those who regularly use the encryption capability have learned to accept the degraded voice quality. Users have also complained of a reduction in range when using encryption. These are known technical issues affecting analog radio systems when digital encryption is introduced. The impact of these problems can be lessened but not totally eliminated. Agency personnel mentioned that if a good and cost-effective algorithm is available, and vendor software supports the OTAR feature, the agency will consider using encrypted radios agencywide.

Many vendors advertise that trunked systems are more difficult for scanners to monitor; but it is difficult, not impossible. Although transmissions cannot be overheard on standard radio scanners that rely on analog technology, multiple vendors have developed scanners capable of tracking trunked analog communications. Public safety frequencies are readily available on the Internet and through other sources. In addition, a particular newsgroup has published information on how to use a computer to monitor the trunked radio control channel of a particular product the agency uses.

**Candidate Recommendation:**

Public safety agencies should be made aware that all unencrypted analog communications, voice or data, conventional or trunked, are susceptible to interception and monitoring at any point in a land mobile radio system. Only the use of encryption will ensure a high degree of voice communications confidentiality and integrity. Regular use of encrypted radios can enhance user confidence. Nonetheless, it is imperative that agencies ensure that security mechanisms will not significantly interfere with operations. If it is feasible, the agency should consider upgrading analog voice communications to digital voice communications. Digital encryption will provide improved audio quality and the coverage area would be comparable with coverage for clear voice. The encryption mechanism should be Federal Information Processing Standard (FIPS) 140-1 compliant for Type 3 systems.

### 4.1.7 Encryption Key Is Not Changed Regularly

An encryption key change represents a significant logistics challenge for the radio system manager, who has to physically "touch" all 300 radios to load a new key. Therefore, the encryption key is not changed regularly due to the resource strain required. An encryption key

that is not changed regularly provides an added vulnerability that could provide increased opportunities to compromise the encryption algorithm, resulting in unauthorized monitoring of critical communications. The agency personnel acknowledged that OTAR would be the best solution to change the encryption key regularly, which would likely increase the utilization of encrypted communications. However, the current system does not support OTAR.

**Candidate Recommendations:**

The OTAR feature allows radios to be rekeyed or zeroized from a remote location. This would eliminate the need to load keys manually via the key variable loader. If the agency considers OTAR, it should first perform a cost/benefit analysis based on the criticality and sensitivity level of the information transmitted among radios. When OTAR is used, the agency should be aware of possible vulnerabilities introduced by the method, and implement and enforce appropriate security features to ensure that all key material is generated, distributed, stored, and destroyed in a secure and controlled manner.

### 4.1.8 Mobile Data Are Transmitted in Clear Mode

Sensitive data (e.g., criminal and privacy information) are transferred unencrypted between mobile vehicles and local and national databases. This information is used by public safety agencies to obtain listings on license plates, drivers' status, stolen vehicle checks, and checks for wanted/missing individuals. Users access the mobile data through laptops located in fleet vehicles. Access to the laptop is controlled through user ID and password; access to the databases is controlled through badge number and car number. Users are automatically logged out 12 hours after they log in to the databases. Users without laptops obtain database information through dispatchers who access the databases from their dispatch consoles and then transmit the query response over the voice radio system.

Data transmitted include the following types of information:

- Driver's license information
- Motor vehicle information
- National Crime Information Center data
- State wanted/stolen data.

Attackers may convert a proprietary mobile data protocol to intercept and interpret mobile data transmissions. It is believed that unencrypted mobile computer terminal (MCT) traffic is no more secure than unencrypted voice traffic. As has occurred with the development of trunking scanners, it appears that devices and software will become available to the general public to enable MCT traffic to be easily monitored.

**Candidate Recommendation:**

Agencies using MCTs to communicate sensitive information over unencrypted channels may want to consider employing encryption techniques. Eventually, methods for monitoring unencrypted MCT traffic will be publicly available. The use of end-to-end encryption can lessen the probability of public safety communications being intercepted by unauthorized personnel.

When procuring wireless data services through commercial providers offering "encryption," agencies should ensure that the type and level of encryption being offered are in accordance with applicable FIPS publications (e.g. FIPS 140-1, FIPS 46-2, NAS Specification V23-94-1).

## 4.2 Best Security Practices

The "best security practices" presented in this section include concepts, designs, and procedures that appear to be reasonable methods of mitigating security risks to public safety communications infrastructures. Each best practice includes a description of the practice and the threat(s) that it counters.

### 4.2.1 Contingency or Disaster Recovery Plan Exists

The radio system is designed to provide a fault tolerance feature that makes the system reliable in various system failure situations. Should a problem develop, it will not affect the basic trunking operation and will not propagate to another part of the system. Should a base station fail, the network management system will detect the failure, send an alarm to the system manager, then eliminate that station from the pool of available channels. If the network management system should fail, the system will still continue trunked operation while losing some of the lesser used features (e.g., dynamic regrouping). If the control channel is jammed, it alarms the network management system.

The system has a backup site that is collocated with the CC. If the primary site fails, the system will be manually switched to be operated from the backup site. The backup site contains a prime site controller in cold standby mode. The site is activated if the primary site goes down. The cold standby system's subscriber database is kept current with the primary RF site database to ensure that operations are minimally affected when the backup site assumes control.

The agency has recently developed contingency plans for Y2K related disruptions. These plans describe the possible failure modes and the impact such failures would have on their operations. The possible failure scenarios include failure of public service power, failure of the telephone system, total or partial failure of the trunked radio system, paging system failure, and microwave system failure. The contingency plans detail a suitable backup plan for use in the event of such failures. The contingency plans have not been tested; however, they should be tested before year 2000.

### 4.2.2 Self-Contained Maintenance Capability Exists

The agency operates its own maintenance facility that provides radio component repair and programs the features, functions, and talkgroup templates into radios. Talkgroup template construction, including feature configuration, is performed only by radio technicians who have extensive experience in radio communications, and who have passed a criminal background investigation.

By maintaining its own facility, the agency has exclusive responsibility for operation, management, and maintenance of the radio equipment, including features and functions. During normal work hours, users bring radios to be repaired to the maintenance facility; after work hours, users coordinate with personnel at the CC, which is staffed 24 hours.

### 4.2.3 The Radio System Has Strict Configuration Management

When radios are programmed or reprogrammed, radio maintenance forms are generated to ensure radio parameters are set correctly. These forms are reviewed by the system managers regularly. Talkgroups are assigned by unit/fleet/subfleet by using a proprietary software that provides the capability to assign structured talkgroups. There are 673 talkgroups in use, with approximately 2,000 available. Controlling talkgroups programmed into the radios ensures safe and efficient operation. The talkgroup templates will be modified to be compliant with Y2K issues, which may require that new templates be created. These changes will be performed by specialized radio technicians.

Radios no longer needed are deprogrammed at the maintenance facility before they are put on auction to ensure that no information is available to unauthorized personnel. Lost and stolen radios are disabled over the air to ensure that unauthorized use is minimized.

### 4.2.4 Data Are Backed Up Regularly

System data that are integral to controlling and monitoring the radio communications system are backed up regularly. The network management system is backed up twice a month; the data system is backed up once a month. This practice allows agency personnel to restore data in a timely manner if they are lost due to system malfunction or if files are destroyed maliciously or accidently.

### 4.2.5 Adequate Access Controls to the Radio Communications System Exist

Security of a radio system can be enforced through user IDs and passwords, different privilege levels, and system activity auditing. Currently, access to the radio system is controlled through user ID and password, although stronger password constraints should be implemented (see Section 4.1.1). In addition, access to the radio system is restricted to a limited number of personnel who have different levels of access privileges. Only two people have administrative

accounts for the operating system to configure security features provided by the operating system. They are responsible for ensuring that system parameters are set correctly, verifying the need for user access, and controlling system privileges.

The system records all system traffic and generates activity tracking reports. The system logs all the activities performed on the system through the network control terminal and dial-in modems. Each activity records time and date of the event, user ID, and type of event (e.g., what program is accessed). Network access from MCTs is also logged in to the data system. The information recorded in the log includes time and date of the event, badge number, and car number. These activity tracking reports are reviewed regularly by the radio system manager.

### 4.2.6 Router Is Configured to Accept Only Specific IP Addresses

The network management system can be accessed through the network control terminal at the maintenance facility or dial-in modems. The router, located at the agency's headquarters, is configured to accept only specific IP addresses. The LAN connected to the router runs limited network resources. In addition, access to the router is restricted to a limited number of people at the headquarters and controlled through user ID and password.

### 4.2.7 Adequate Environmental Controls Are in Place

The facilities housing radio equipment have adequate environmental controls installed and operational. These controls are—

- Fire extinguishers
- Heat and smoke detectors
- Uninterruptible power supplies
- Emergency power provided by auxiliary generators with fuel to operate for extended periods
- Emergency switch and emergency shutdown procedures
- Grounding to protect the sites against lightning hits.

# 5. SUMMARY

The security issues identified during the third site visit are documented in Section 4 and are summarized as follow:

- No consolidated security policy or procedures exist
- An off-site storage facility has not been designated for backup tapes
- Physical security at several radio sites needs improvement
- Logical unit IDs are manually assigned
- Dial-in modems for the radio communications system could be exploited
- Encryption capable radios are not always used in encryption mode
- Encryption key is not changed regularly
- Mobile data are transmitted in clear mode.

The security issues identified are related to administrative and management, physical, and communications security. Developing and exercising plans, procedures, and policies that specify security processes and provide detailed guidance to agency staff will reinforce the need for security to agency staff and help identify areas in which security can be improved. Controlling access to the facility or CC is one way to easily provide a first level of protection to the radio system components. Dial-in access to the system increases the risk of unauthorized personnel accessing the system; therefore, more stringent security mechanisms should be implemented. As stated in Section 4.1.6, trunk-tracking scanners are readily available. Although the content of MCT messages is not easily discerned, the ability exists to convert the content of such messages. Eventually, a method will be developed to make that content understandable. Therefore, mobile data transmissions should be encrypted.

# APPENDIX A

# ACRONYMS

| | |
|---|---|
| CAD | Computer-Aided Dispatch |
| CC | Communications Center |
| CCTV | Closed Circuit Television |
| EMS | Emergency Medical Services |
| FIPS | Federal Information Processing Standard |
| GHz | Gigahertz |
| ID | Identification |
| kHz | kilohertz |
| LAN | Local Area Network |
| MDT | Mobile Data Terminal |
| MHz | Megahertz |
| NCC | Network Control Center |
| OTAR | Over-the-Air-Rekeying |
| PMO | Program Management Office |
| PSWN | Public Safety Wireless Network |
| PTT | Push-to-Talk |
| RF | Radio Frequency |
| TIA/EIA | Telecommunications Industry Association/Electronics Industry Association |
| Y2K | Year 2000 |

# APPENDIX B

# SECURITY FIELD DATA COLLECTION PLAN

# Security Field Data Collection Plan

## 1.0 INTRODUCTION

A series of security field data collection and analysis efforts is being conducted with the primary goals of identifying security issues and concerns associated with evolving digital land mobile radio (DLMR) systems. This *Security Field Data Collection Plan* was developed to ensure consistency and adequate coverage across the organizations at which data is being collected.

## 2.0 APPROACH

The following steps outline the high level approach used in conducting each security field data collection and analysis effort.

### Step 1: Coordinate and prepare for the data collection effort

- Identify personnel for conducting the security data collection effort
- Coordinate the data collection schedule with the organization
- Determine which organization personnel should be interviewed
- Identify the type of system components at the organization for pre-interview research
- Ask for documentation containing descriptions of the identified system components and system diagrams
- Provide the organization point of contact with the Security Field Data Collection Plan security questions and background information.

### Step 2: Collect system and organization data

- Collect data by reviewing the documents and diagrams provided by the organization
- Visit the organization and interview personnel using the data collection plan interview guide
- Validate the collected data
- Tour facility and observe operating environment

- Collect additional system and security information
- Identify current security practices, concerns, and needs.

**Step 3: Research and clarify data gathered from the organization**

- Conduct research on security issues and concerns raised
- Recontact the organization, if necessary, to clarify information gathered.

**Step 4: Analyze and document security issues, candidate recommendations, and best practices**

- Describe the security issues raised during data collection
- Provide candidate countermeasure recommendations for security issues
- Document existing best practices at the organization
- Consolidate the organization data, analysis, and recommendations into a report.

## 3.0 SECURITY QUESTIONS

The security questions found on the following pages are categorized as follows:

- General
- Administrative security
- Physical security
- Automated information system (AIS) and network security
- Communications security
- Portable/mobile radios
- Portable/mobile data
- Other.

These questions serve as guidelines to the interviewer. It is expected that discussions will expand upon these questions. A glossary is provided at the end of this plan to help clarify terms used in the questions.

| GENERAL |
| --- |
| Agency/Organization:<br>Agency Contact:<br>Job Title/Function:<br>Telephone Number/Fax Number: |
| System operations:<br>• Number of users/radios<br>• Coverage (county, state)<br>• Types of users (police, fire, EMS, other)<br>• Number of dispatch centers/dispatch positions at each center<br>• Number of dispatchers per shift<br>• Number of channels and frequencies |
| Type of equipment used:<br><br>Manufacturer of radio system<br><br>Product name<br><br>Type of services:<br>• Encryption<br>• Voice and data capability<br>• Agencies using mobile data<br>• Paging capability |
| Sensitivity of voice/data stored, processed, or transmitted? (Confidentiality, Integrity requirements)<br><br>Mission criticality of operations? (Availability requirements) |
| May we obtain a high-level system diagram, even if hand drawn? |

## ADMINISTRATIVE MANAGEMENT

### Security Policy

Does a written security plan exist for the RF network and any wireline networks or systems?

What kind of information does the security plan contain?

Who is responsible for reading and maintaining the security plan?

Does a written security policy exist for the organization?

If yes, does this policy cover AIS and radio systems?

If yes, is the policy consistently enforced?

If yes, may we obtain a copy of the written policy?

Has any type of security evaluation or security testing been performed at the organization?
If yes, when was the last time an ST&E was conducted?

May we obtain a copy of the ST&E report?

### Contingency Plans

Is there a contingency plan?

If yes, what is the scope of the contingency plan?

Is the contingency plan tested periodically and updated?

When was the last time the contingency plan was tested and updated?

Is there any redundancy available for consoles and communications connectivity?

Is the system capable of operating in a degraded state, if necessary? Please describe.

Is there a "ready-to-use" site designated in case of unavailability of the primary site?

Where is the "ready-to-use" site located?

| ADMINISTRATIVE MANAGEMENT |
|---|
| Do contingency operations (i.e., emergency sites and equipment) provide the same level of security controls as regular operations? |
| **Data Backup** |
| Are the system/network data and resources backed up periodically?<br>• How often are they backed up? (Incremental backup/full backup)<br>• Is there an off-site storage facility for backup media?<br>• How often are the backup media sent to the off-site facility? |
| **Configuration Management** |
| Is there configuration management of computer programs?<br><br>Who is responsible for reviewing and approving any changes made?<br><br>Are all changes made to the system documented? |
| **Security Training** |
| Are users provided security training?<br><br>How often do they receive security training?<br><br>What subjects does the security training cover?<br><br>What methods are used to provide security training (e.g., sessions, memorandums)? |

## ADMINISTRATIVE MANAGEMENT

### Personnel Security

Is a personnel security policy established?

Is a background check required for users (e.g., employees, contractors) prior to gaining access to the system?

Is a background check required for cleaning and maintenance personnel prior to being hired?

Is there any additional or more detailed check required for administrators of the system?

Are contractors and support personnel (e.g., cleaning, vending, maintenance personnel) subject to the same check as users and/or administrators?

### Maintenance/Services

Does the organization own the maintenance facilities?

Who performs equipment maintenance services?

What type of maintenance services are performed?

Are maintenance activities monitored to ensure security?

Is DLMR equipment transported to and from maintenance locations in a secure manner?

Is equipment tested after being serviced to ensure that security controls or functions have not been tampered with?

Are all maintenance activities recorded?

Is the maintenance record kept for a specified period of time?

## PHYSICAL

### Facility

Is a physical security officer designated in writing?

How are the facility perimeters protected?

Who has access to the communications system facilities during duty hours?

How is access to facilities controlled during duty hours?

Is there access control at the facility entry (guards/locks)?

Who has the building master keys for the facilities?

Are visitors logged in and out?

Are bags searched upon entry (even if random)?

Are bags searched upon exit (even if random)?

Are identification badges required for access?

Are visitors required to wear badges at all times?

Are visitors escorted at all times?

Is surveillance equipment used?

How is access to facilities controlled after duty hours?

Who has access to the facilities after duty hours?

### Computer Room(s)

What computer room(s) exist to manage and support the organization's communications?

- What are the functions of each?
- Where are they located?
- What type of computer equipment does each computer room house?

| PHYSICAL |
| --- |
| Who has access to the computer rooms?<br><br>How are the areas secured where computer equipment is stored?<br><br>Are doors locked at all times?<br><br>Are cipher locks used? If so, where/under what conditions?<br><br>If cipher locks are used, are the combinations changed regularly? When?<br><br>Are visitors logged in and out?<br>Are visitors escorted at all times?<br><br>Are computer rooms manned 24 hours a day, 7 days a week? |
| **Dispatch Center** |
| Who has access to the dispatch center?<br><br>What physical security measures (e.g., guards, keys, access cards) are used to prevent unauthorized access to the dispatch center?<br><br>Are doors locked at all times?<br><br>Are cipher locks used? If so, where/under what conditions?<br><br>If cipher locks are used, are the combinations changed regularly? When?<br><br>Are visitors logged in and out?<br><br>Are visitors escorted at all times?<br><br>Is surveillance equipment used? |
| **Radio Sites** |
| Who has access to the radio sites? |

| PHYSICAL |
| --- |
| Are physical access control measures used to prevent unauthorized access to the sites' perimeters and shelters ?<br><br>Are the radio sites collocated with other agencies, contractors, or commercial organizations?<br><br>If yes, what are the physical security measures used to control the shared sites?<br><br>Do the sites comply with any physical security requirements set forth in the specified regulations (e.g., county jurisdiction code)?<br><br>Do physical access control devices activate alarms at a central location or local police department?<br><br>Are sites regularly inspected by authorized personnel?<br><br>Are the site locations published?<br><br>Are the heat and humidity alarms installed? |
| **Telephone Closet** |
| Who has access to the telephone closet?<br><br>Are doors locked at all times?<br><br>Are keys changed regularly? When? |
| **Environmental** |
| What environmental controls are in place to protect the system and the facility under emergency conditions?<br>• Are heat and smoke detectors installed in the ceilings and under raised floors?<br>• Is there a fire alarm?<br>• Is there a fire suppression system?<br>• Is the fire suppression system tested periodically?<br>• Is there a raised floor?<br>• Are there uninterruptible power supplies? |

| PHYSICAL |
| --- |
| • Is there an emergency power capability?<br>• Is there a procedure to ensure that fuel running the auxiliary generators is sufficient and not contaminated?<br>• Is there an emergency switch and emergency shutdown procedures?<br>• Is the air conditioning system dedicated to the dispatch center or to the computer room?<br>• Is backup air conditioning available?<br>• Is proper grounding provided?<br>• Are the radio sites properly installed to protect against lightning?<br><br>• Is alternate routing available for power and phone services? |

## AIS/NETWORK (System/Network Administrators)

***** Note *****

**This section addresses the questions for system/network administrators responsible for managing any wireline system or network that interfaces with the RF network.**

### Identification and Authentication

Are there procedures established to manage authorized user accounts on the system/network (e.g., create, delete, disable)?

How are user accounts/passwords distributed?

Identify any password constraints used by your system:

- Password length
- Password composition
- Password aging (How often must passwords be changed?)
- Password history (Are old passwords prohibited from reuse for a certain time period?)
- Change of initial password
- Resetting of forgotten passwords (Is a change then required?)
- User account locked out after a specified number of unsuccessful login attempts.

Are there procedures for handling accounts for users no longer requiring access to the system or network?

Is a list of user accounts maintained, reviewed, and updated? How often?

### Access Control

Are there different levels of access to the system/network (e.g., users, system/network administrator, security administrator)?

What kind of privileges does each level have?

How are user's access privileges to the system or its data determined?

Is there network-based remote access to the local area network (e.g., Internet, Intranet, WAN)?

| AIS/NETWORK (System/Network Administrators) |
|---|
| **Audit** |
| Are audit trails available? (electronic logs of security related events performed by system users)<br><br>What kinds of security events are recorded in the audit trails?<br><br>Who reviews the audit trails? How often?<br><br>Are security activities on network hosts recorded? If so, who reviews? How often? |
| **Remote Dial-in Access** |
| Is there any dial-in access to the network? If so,<br><br>• Who has dial-in access to the system/network?<br><br>• To what components is dial-in access allowed?<br><br>• What functions are performed remotely?<br><br>• Are there any security controls for the remote access? (e.g., dial-back modem, strong authentication)<br><br>• Are there constraints for failed access attempts?<br><br>– How many times is failed access allowed?<br><br>– What occurs if the number of failed accesses is exceeded?<br><br>Is a list of user accounts for dial-in access maintained, reviewed, and updated? How often? |
| **Other** |
| Is any virus protection provided for the components that are a part of the system/network? |

**AIS/NETWORK (System Users)**

***** Note *****

**This section addresses the questions for system users that access the system/network to perform their functions.**

**Identification and Authentication**

Are you required to present your ID and password before you access the system/network?

Who assigns your ID and initial password?

Do you change your initial password at the first login?

How often do you change your password?

Are there policies or procedures for selecting passwords?

What is the minimum length of a password?

Are you required to select a combination of alphabetic and numeric characters for your password?

Does the system/network notify you of the need to change your password?

Are there procedures for reporting forgotten passwords?

If you forgot your password, who do you contact to receive your password?

- Is your password the same password you used or do you receive a default password?
- If you receive a default password, do you need to change the password immediately?

Are there procedures for reporting security incidents?

Do you know how many attempts you are allowed to enter your user ID or password before your account is disabled?

| AIS/NETWORK (System Users) |
|---|
| Are there procedures for reporting that your account is disabled? |
| **Access Control** |
| What are your responsibilities for controlling access to information on the system?<br><br>Are you restricted to accessing only applications necessary for your job functions?<br><br>If not, what other applications are you able to access?<br><br>Is your terminal disconnected after an extended period of inactivity?<br><br>Do you log out when you leave your terminal unattended? |
| **Remote Dial-in Access** |
| Do you have dial-in access to the system?<br><br>What functions do you perform remotely?<br><br>Are you required to use your ID and password for dial-in access?<br><br>Who assigns your ID and password for dial-in access?<br><br>How often do you change your password ? |
| **Other** |
| Do you run anti-virus software regularly?<br><br>What would you do if you identified a virus on your system? |

| COMMUNICATIONS |
|---|
| **Encryption** |
| Is encryption provided to protect data transported among the system components?<br><br>What type of encryption is used?<br><br>Is encryption method documented and approved?<br><br>Is the control channel encrypted?<br><br>If no, do you have concerns about an unencrypted control channel being used to exploit radio communications?<br><br>In an emergency situation, how is sensitive information transmitted (via a clear channel or an encrypted channel)? |
| **Key Management** |
| Are written guidelines established for the handling and safeguarding of keying materials?<br><br>What is the key lifetime?<br><br>How are encryption keys changed?<br><br>How are key loaders protected?<br><br>How are radios with the current key loaded protected?<br><br>Are there procedures for protecting keys during their life cycle (e.g., generation, distribution, storage, destruction)?<br><br>When keys are compromised, are they destroyed in a secure manner? |
| **Redundancy** |
| Is an alternative communications path available in case a primary path fails?<br><br>Is there adequate backup (spare) communications equipment available? |
| **Emission Security** |
| When the system was designed, had emission security been considered?<br><br>Do you have concerns about electronic emissions being compromised and used to exploit the radio system? |

| RADIO (Portable/Mobile) |
|---|
| **User Verification** |
| Does the radio authenticate the currently assigned user?<br><br>Do the radio system components authenticate themselves to one another to ensure that only valid radios may be used?<br><br>What are the procedures for managing system users?<br><br>What are the procedures for managing talkgroups or channel assignments?<br><br>• Who assigns users to talkgroups?<br><br>• How are talkgroups assigned? by function?<br><br>• How are channels assigned? (by function?) |
| **Encryption** |
| Is encryption provided for radio equipment?<br><br>What percentage of mobiles and portables have data?<br><br>What type of encryption is used?<br><br>Is the encryption on the radio system transparent (e.g., uses end-to-end encryption)?<br><br>Are there policies and procedures to enforce the use of the encryption feature?<br><br>Do you use the encryption feature?<br><br>Do you turn this feature on and off?<br><br>Have you experienced any impact on operations due to the use of encryption (e.g., minimized range, degraded voice quality)?<br><br>Are multi-encryption modes implemented to meet an interoperable need?<br><br>Have you experienced any interoperability problems due to the use of incompatible encryption schemes between your system and others? |

Have the cryptographic components used in the system been FIPS 140-1 certified?

If you don't use encryption, what are the reasons that you don't use it?

**Over-the-Air-Rekeying**

Do you currently use over-the-air-rekeying (OTAR)?

- If yes, how is OTAR managed?

- How many people are authorized to manage rekeying?

**Remote Dial-in Access**

Who has dial-in access?

To what components is dial-in access allowed?

What functions are performed remotely?

Are there any security controls for the remote access? (e.g., dial-back modem, strong authentication)

Are there constraints for failed access attempts?

How many times is failed access allowed?

What occurs if the number of failed accesses is exceeded?

**Redundancy**

Is any redundancy available for dispatch consoles and RF network connectivity?

**Lost and Stolen Radio**

What are the procedures for handling lost or stolen radios?

How is the loss reported to radio managers?

Is there a capability to disable such radios?

If such radios contain encryption capabilities, is any different action taken upon their loss than that taken for non-encryption capable radios?

Are procedures established for controlling access to MDTs and radios?

What are the procedures for activating radios recovered from being lost or stolen?

Are procedures in place for the secure disposal/destruction of radios?

Are procedures established for use of the emergency activation button?

| Portable/Mobile Data |
| --- |
| Does your organization utilize data communications?<br><br>What type of MDTs, MCTs, laptops, or portable data terminals used?<br><br>Is the data encrypted?<br><br>What type of services does the MDT/MCT provide? (e.g., data query, e-mail)<br><br>Do you use a commercial (commercial service) data communication system?<br><br>Is data connectivity to other systems, such as National Crime Information Center (NCIC), over dedicated, leased lines or public switched telephone networks?<br><br>Do your data communications share bandwidth with the voice communications? If not, how are they distinct?<br><br>Does the MDT/MCT provide you with capabilities of accessing a system/network?<br>• If yes, are you required to identify yourself before accessing the network/system?<br>• What kinds of authentication mechanisms are used (e.g., password, personal identification number)?<br>• Are there any authentication constraints used to prevent unauthorized access?<br>• Is user account locked out after a specified number of unsuccessful login attempts?<br>• Are there procedures for requesting your account be unlocked?<br>User account management<br>• Are there procedures established to manage authorized user accounts on MDT/MCT (e.g., create, delete, disable)? |

| Portable/Mobile Data |
| --- |
| • Are there procedures for handling accounts for users no longer requiring access to the MDT/MCT?<br><br>• Is a list of user accounts maintained, reviewed, and updated? How often?<br><br>Is any anti-virus protection provided for the MDTs/MCTs? |
| **Property Disposal** |
| Are procedures in place for the secure disposal/destruction of MDTs/MCTs?<br><br>Is all organization/operation's specific data removed from the device?<br><br>For an MDT/MCT that is no longer used by the organization, is information that would allow continued access to the organization's system or data deleted from the central controller (e.g., unit number, identity code)? |

## OTHER

Do you have any concerns about the security of your voice communications? If so, please explain.

Do you have any concerns about the security of your data communications? If so, please explain.

Have there been any incidents concerning the confidentiality, availability, or integrity of your voice or data systems? If so, please explain.

Please provide information on any other issues or concerns that you have concerning voice and data system security.

# GLOSSARY

**Access Control**

A technique used to define or restrict the rights or capabilities of individuals or application programs to communicate with other individuals or application programs 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 Information System**

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

**Availability**

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

**Communications Security**

Protection measures to protect data that is transferred using communication lines. This includes ensuring that transactions are not invalid, incomplete, or altered.

**Computer Room**

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

**Confidentiality**

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

**Configuration Management**

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

**Contingency Plan**

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

**Emission Security**

Measures to control decipherable electronic signals unintentionally emitted from an information system and communications equipment.

**Encryption**

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

**Identification**

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

**Integrity**

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

**Jamming**

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

**Key**

When used in the context of encryption, a series of numbers which are used by an encryption algorithm to transform plain text data into encrypted (cipher text) data, and vice versa.

**Key Management**

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

**Land Mobile Radio**

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

**Mobile Data Terminal**

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

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

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

**Password**

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

**Security Plan**

A document which depicts a site's plan for securing its system.

**Virus**

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

**Vulnerability**

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