PUBLIC SAFETY

PSWN PROGRAM

WIRELESS NETWORK

Saving Lives and Property Through Improved Interoperability

Operational Best Practices for Managing Trunked Land Mobile Radio Systems

Final

May 2003

Table of Contents

Page

1. INTRODUCTION 1

1.2 Scope 1
1.3 Background 2
1.4 Document Organization 2

2. METHODOLOGY 4

3. KEY CONSIDERATIONS OVERVIEW 5

4. BEST PRACTICES ASSESSMENT 7

4.1 Technical Best Practices 8
4.2 Operational Best Practices 12
4.2.1 Talk Group Organization 13
4.2.2 System Administration 14
4.2.3 Interoperability 17
4.2.4 Training 19
4.3 Political Best Practices 21

5. LESSONS LEARNED ASSESSMENT 23

6. CONSIDERATIONS AND CONCLUSIONS 28

APPENDIX A—TRUNKING OVERVIEW A-1

APPENDIX B—DATA COLLECTION MATERIALS B-1

APPENDIX C—OPERATING ENVIRONMENT OVERVIEW C-1

APPENDIX D—KEY TECHNICAL CONSIDERATIONS D-1

D.1 Capacity 1
D.2 Security 1
D.3 Trunking Protocols 3

APPENDIX E—KEY OPERATIONAL CONSIDERATIONS E-1

E.1 Talk Group Organization 1
E.2 System Administration 4
E.3 Interoperability 8
E.4 Training 12

APPENDIX F—KEY POLITICAL ARENA CONSIDERATIONS F-1

F.1 Coordination 1
F.2 Resource Sharing 2
F.3 Stakeholder Support 2

APPENDIX G—PROJECT 25 ..... G-1

APPENDIX H—LIST OF ACRONYMS H-1

1. INTRODUCTION

Until about 30 years ago, public safety agencies relied heavily on conventional radio systems. Trunked LMR systems became popular as the population in urban areas grew and the size and scope of public safety missions and requirements expanded, resulting in a greater demand for public safety spectrum to meet communications needs. In effect, trunked LMR systems took precedence in urban areas because of the technology's efficient use of finite public safety spectrum through frequency sharing. Today, trunked LMR systems are common within the public safety arena because of this benefit, as well as other advantages including fast system access, enhanced feature sets, channel efficiency, security, and flexibility. In short, trunking technology provides the ability to easily and efficiently segment the user population of an organization into functional groups that are more reflective of the actual organizational structure of the user agency. These groups are typically referred to as talk groups.[1] This segmentation allows the routing of calls to members of only these groups. Despite these technological benefits, trunked LMR systems require communications officials to coordinate, manage, and consistently monitor several aspects of the system as well to plan as for future improvements. With the aid of this *Operational Best Practices for Managing Trunked LMR Systems*, communications officials may be able to identify new procedures or improved methods to complement system management functions and assist users with LMR communications. It is important to note that despite this report's focus on trunking technology, communications, officials that manage systems using alternate technologies may also find many of the practices outlined are applicable to their LMR system operations. For readers desiring an overview of the basics of trunking technology, see Appendix A.

Trunked land mobile radio (LMR) system oversight requires a multifaceted management approach. Communications officials routinely must assess various technical and operational factors that impact their systems, and ultimately their customers, the radio users. Yet, LMR operational factors are seldom subjected to further research and documentation. To assist communications officials with this important endeavor, the Public Safety Wireless Network (PSWN) Program has developed the *Operational Best Practices for Managing Trunked LMR Systems* document. This report explores and documents various operational techniques, procedures, and processes that may be helpful to system managers and users alike. It highlights best practices and lessons learned that, when implemented, may result in enhanced interoperability, improved system efficiencies, and the advancement of overall LMR management functions. This report is intended to support public safety radio system managers, communications representatives, or project managers researching procedures and activities for improved trunked LMR capabilities.

1.2 Scope

Operational Best Practices for Managing Trunked LMR Systems is based on an examination of the LMR operational environment of several public safety organizations across the Nation. The objective of the report is to document best practices and lessons learned for talk group design as they relate to interoperability and to the overall management of trunked LMR systems. Interviewees represent a diverse set of communications officials responsible for small, medium, and large LMR systems within metropolitan, suburban, and rural areas. For the

[1] A talk group is a preprogrammed, predetermined basic organizational group of LMR users.

purposes of this report, system size is categorized according to the total radio user population as shown in Table 1.

Table 1
LMR System Size

System Size	Radio User Population
Small	Fewer than 5,000
Medium	5,000—10,000
Large	More than 10,000

This report offers a key point of reference regarding available technical, operational, or managerial capabilities that could be leveraged to support trunked LMR systems.

1.3 Background

The PSWN Program's *How To Guide for Establishing and Managing Talk Groups* introduced a high-level strategic process divided into four components—capturing operational requirements, reviewing system capabilities, establishing the talk group plan, and managing talk groups. Building on the *How To Guide*, this report will detail best practices and lessons learned for several areas within each component of that process. As a result, this companion report will provide an operational and managerial perspective of trunked LMR systems with specific actions for increasing interoperability opportunities.

1.4 Document Organization

This report was developed to identify operational best practices and lessons learned regarding the oversight of trunked LMR systems. It is organized in the following sections—

- Section 1—highlights the purpose and background of this effort.
- Section 2—details the process used to develop the report.
- Section 3—introduces the key technical, operational, and political considerations used to baseline the communications environment of public safety trunked LMR users.
- Section 4—features the best practices for the oversight of trunked LMR systems.
- Section 5—features the lessons learned for the oversight of trunked LMR systems.
- Section 6—provides a concluding summary that can be used by system managers to support interoperability and management enhancements for their respective systems.
- Appendix A—provides a technical description of trunking and talk groups and discusses the advantage and disadvantages of trunked radio systems.

- Appendix B—contains the materials used for the data collection effort for this report, including the survey guide and interview list.

- Appendix C—provides an operational overview of the various agencies consulted for this study.

- Appendix D—provides a detailed explanation of the key technical considerations for trunked LMR systems.

- Appendix E—contains information regarding the key operational considerations for managing trunked LMR systems.

- Appendix F—explains the political arena that influences the management of trunked radio systems.

- Appendix G—provides an overview of Project 25 (P25) and discusses its impact on interoperability

- Appendix H—contains a list of the acronyms used in this report.

2. METHODOLOGY

To develop this *Operational Best Practices for Managing Trunked LMR Systems*, the PSWN Program conducted a targeted assessment of the current operational environment of public safety communications. The assessment process, as shown in Figure 1, included planning and advance preparations, a data-gathering effort, an analysis of interview data and related documentation, and an analysis of best practices and lessons learned. The initial phase in the process, planning and advance preparations, comprises the identification of public safety agencies and the development of an interview guide. The interview guide, included in Appendix B, targets various components of LMR systems and their usage, including talk group organization, operations, interoperability, and general system administration. Using these guides, the data collection team held interviews with public safety senior executives, technical representatives, and communications center personnel. The data collection team also conducted site visits to communications centers and radio workshops, where appropriate. Appendix C presents an overview of the operating environments of the agencies studied. During the data analysis phase, several important tasks were completed, including the identification of key technical, operational, and political baseline considerations. These considerations served as the basis for the review and analysis of the data collection results. After an analysis of the data, several common themes became evident. These themes became the foundation for the final sections, Best Practices (Section 4) and Lessons Learned (Section 5).

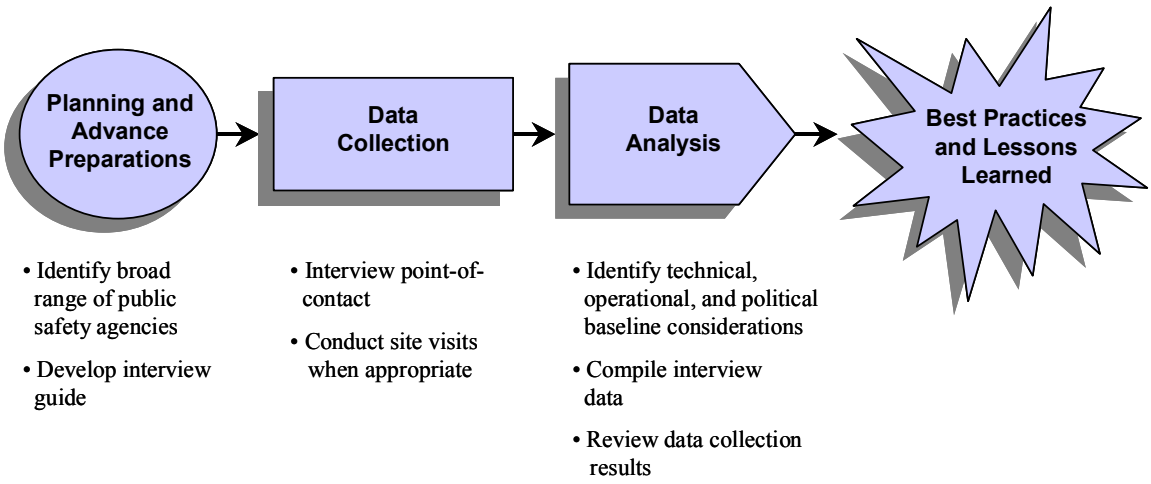


Figure 1
Baseline Assessment Model

3. KEY CONSIDERATIONS OVERVIEW

Determining the optimal means by which public safety agencies design, manage, and maintain LMR systems is often challenging and time consuming due to the dynamic nature of the public safety environment. Therefore, it is critical that public safety officials at the system manager level are equipped with the proper tools. To assist in this effort, a number of key considerations yielding common challenges for system managers were identified. As illustrated in Figure 2 and detailed in Appendices D, E, and F, these considerations are grouped into three focus areas—technical environment, operational environment, and the political arena. Collectively, these focus areas encompass the framework for addressing trunked radio system management, improving interoperability, and maximizing system efficiency.

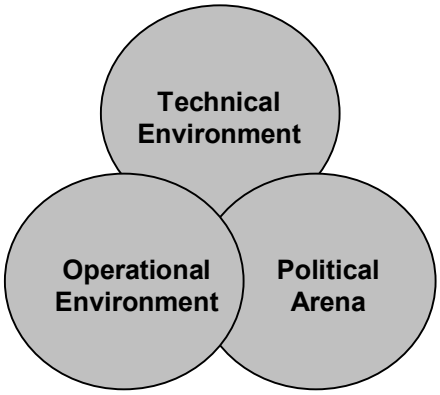
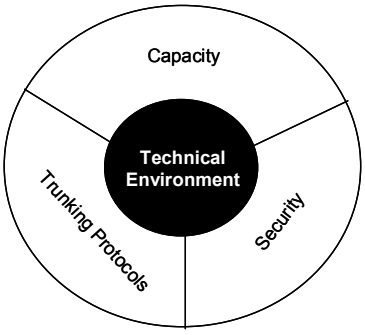


Figure 2
Focus Areas

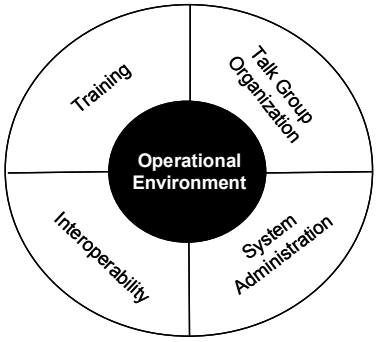
Within each of the focus areas, sub-elements are identified. The following paragraphs further describe these sub-elements.

Technical Environment



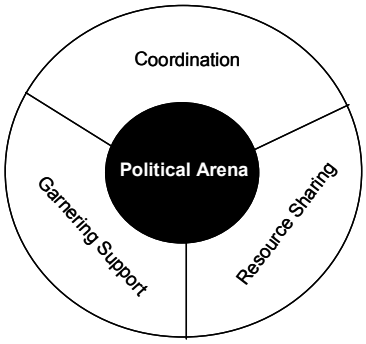
Various technical advantages are associated with installing a trunked radio system. Regardless of the system manufacturer, three common system features emerged as having an operational impact including capacity, security, and trunking protocols. Appendix D details each of these sub-elements.

Operational Environment



Operationally, public safety agencies face an array of challenges relating to system management. These challenges stem from both current and future operational needs that must be addressed to ensure the availability of communications. A number of operational considerations are identified as significant to trunked radio systems operations. Specifically, these operational considerations include—talk group organization, system administration, interoperability, and training. Appendix E details each of these operational considerations.

Political Arena



The public safety political arena is filled with implications for the radio user, technician, and stakeholder. Regardless of technology, the political environment influences the planning, implementation, maintenance, and future of an LMR system. More importantly, the political environment impacts the approach public safety organizations take in establishing or improving wireless interoperability. Specifically, this approach, which is detailed in Appendix F, involves coordinating with other organizations, sharing resources where appropriate, and garnering stakeholder support and user acceptance.

4. BEST PRACTICES ASSESSMENT

This section details the best practices drawn from the experiences of various public safety agencies operating trunked LMR systems. The focus of these best practices is how they relate to overall management of trunked systems, interoperability, and impact on public safety operations. The best practices, summarized in Table 2 and detailed in Sections 4.1, 4.2, and 4.3—grouped into three main categories—technical, operational, and political—highlight innovative and high-impact activities used by a variety of public safety agencies. Note, however, that these best practices may not be suitable or applicable to all agencies. Officials should weigh their respective agency's size, geographic constraints, existing interoperability solutions, and distinct operating practices, prior to implementing any of the best practices identified below.

Table 2
Summary of Best Practices

Consideration	Best Practices
Technical	• Research similar, existing trunked systems
	• Maintain effective existing system operational practices during system migration
	• Test radio features before full deployment
	• Maintain 20 percent excess system channel capacity
	• Institute status messaging (when appropriate)
	• Use the scan function to respond to cross-jurisdictional incidents proactively
	• Regularly monitor land use and urban development
	• Understand the permit, zoning, and building codes for tower sites
	• Consider infrastructure sharing and relationship building with a variety of internal and external agencies and commercial service providers
Operational	*Talk Group Organization*
	• Involve the user community in planning
	• Define a default fleet map
	• Develop a standardized template across domains
	• Regularly review fleet maps and talk group plans
	System Administration
	• Develop a disaster recovery plan
	• Inform dispatchers of system upgrades
	• Create a regional news group
	• Monitor system statistics
	• Track the distribution and maintenance of subscriber units
	• Perform routine system failure testing
	• Develop and implement a formal maintenance plan
	Interoperability
	• Implement special operations or coordination talk groups
	• Match unit numbers and zones when sharing subscriber IDs
	• Consider transportable interoperability solutions to address commercial interference
	Training
	• Establish training teams
	• Survey users to identify systems concerns
	• Develop multiple training delivery formats
	• Employ visual aids

Consideration	Best Practices
Political	• Participate in working groups
	• Share resources
	• Garner stakeholder and user acceptance

4.1 Technical Best Practices

This section describes the best practices associated with the technical environment. Summarized in Table 3 are the technical best practices identified during the course of the study. Also included here are "real world" examples of technical best practices from several agencies across the Nation. Descriptions of each of the agencies (listed as agencies "A" – "L" to ensure anonymity) are detailed in Appendix C.

Table 3
Technical Best Practices

Consideration	Best Practices
Technical	• Research similar, existing trunked systems
	• Maintain effective existing system operational practices during system migration
	• Test radio features before full deployment
	• Maintain 20 percent excess system channel capacity
	• Institute status messaging (when appropriate)
	• Use the scan function to respond to cross-jurisdictional incidents proactively
	• Regularly monitor land use and urban development
	• Understand the permit, zoning, and building codes for tower sites
	• Consider infrastructure sharing and relationship building with a variety of internal and external agencies and commercial service providers

- **Research Similar, Existing Trunked Systems**. A number of public safety agencies have implemented trunked radio systems successfully. When planning a new communications system, agencies should identify others that possess similar operational and demographic characteristics and recognize those practices that have been successful. By researching and possibly visiting regions with trunked systems in place, system managers can determine how other agencies have designed their systems and developed their fleet maps. Moreover, system managers may find it useful to visit areas that have similar interoperability requirements to gain a better understanding of the various methods for achieving interoperability on a trunked system. Furthermore, the system manager may gain a better understanding of what system features are available from various vendors in order to determine an optimal set of system features.

- **Maintain Effective Existing System Operational Practices During System Migration**. Migrating from a conventional radio system to a trunked radio system will likely result in operational changes. These changes, often dependent on organizational mission, may be insignificant or may cause a substantial change in standard operating procedures (SOP). By preserving as many existing operational

practices as possible when migrating to a new system, the change experienced by radio users will be minimized.

Public safety radio users in Agency F were issued two mobile radios while operating on a conventional system. One of the radios is permanently tuned to a designated "emergency channel," which serves as a countywide channel used to issue alerts and inform users of emergency situations. Radio users can only monitor this channel, while dispatchers can broadcast messages via this channel. The other radio serves as a fully functional mobile radio. When migrating to the new trunked system, system managers wanted to maintain the emergency channel, which was an effective operational practice in their county. To ensure this practice continued with the trunked system, system managers worked with their system vendor to design a product tailored to their desires. The product allows the emergency talk group to be monitored continually via a mobile radio.

- **Test Radio Features Before Full Deployment**. User requirements and missions drive the need for various radio features. To save time and money, system managers can test certain radio features (e.g., the order of talk groups in radios, the scan feature) with a test group before distributing radios systemwide. The test group will employ the radios in day-to-day operations to determine operational effectiveness of these features. This practice is especially important in larger agencies where the number of users may be in the thousands and changes to radio features could require a significant number of resources.

Agency J uses test divisions for certain radio features because of the uncertainty associated with newer radio features and the potential impact on day-to-day operations. System managers want to ensure operational effectiveness while determining which features users prefer. After receiving feedback from the test divisions, changes are made and another round of testing occurs. Finally, radios are deployed in the field with user-friendly and operationally effective features.

- **Maintain 20 Percent Excess System Channel Capacity**. With large systems, it is necessary to maintain excess capacity for major, multi-agency responses. Excess capacity will help ease channel congestion and ensure that all users can access the trunked system in a timely manner during a major incident.

A radio manager from Agency H stated that maintaining 20 percent excess channel capacity allowed users to access the system efficiently during a major wild land fire incident. During the incident, the system was busy less than 2 percent of the time, and users were able to access the system within 5 seconds.

Maintaining excess capacity is an ideal practice that may help to ensure that users can quickly access the trunked system during a major incident regardless of system size. However, system managers would need to decide whether purchasing excess capacity is feasible. This practice needs to be well thought through prior to a system purchase. Continual channel capacity evaluation should occur to ensure that the system maintains the desired excess. In some areas, additional channel capacity may be limited, and other alternatives, such as sharing infrastructure (i.e. radio channels) with

other area or regional systems may be the only option to increase capacity. Acquisition of additional spectrum can sometimes be a protracted process that may require substantial time and monetary resources, adversely affecting planning and budgetary efforts.

- **Institute Status Messaging When Appropriate**. Some public safety agencies consider the use of status messaging beneficial because it can reduce voice traffic over a burdened trunked system. A status message is a text message sent via a mobile data computer or terminal to the dispatcher informing the dispatcher of the radio user's whereabouts. Various public safety agencies use status messaging to inform dispatchers of personnel's response status, such as "enroute to scene" or "clear from scene." Status messaging reduces voice communications by off-loading administrative traffic to an alternative technology. Status messaging can be supported efficiently in modern trunked systems without the need to have an alternative system.

Agency E uses status messaging to reduce voice channel congestion. This practice is a SOP for Agency E when responding to an incident. The system manager collects statistics on response times and performance efficiencies related to status messaging. By analyzing this data, the system manager is able to determine performance rates per subscriber ID. When the performance rate falls below a certain percentage, the public safety radio user receives refresher training.

- **Use the Scan Function to Respond to Cross-Jurisdictional Incidents Proactively.** In multi-agency systems, public safety agencies can be proactive in their approach to interoperability by scanning the talk groups of neighboring jurisdictions. Scan is a feature typically included as an option in mobile and portable subscriber units; however, the feature requires setup and additional training. Some types and methods of scanning features will require a "system decision" as well as operational decisions based on appropriate training. For example, when subscriber units are programmed with talk groups from surrounding jurisdictions, public safety officials can identify emergency incidents that may impact their own jurisdiction and initiate a response prior to ever being contacted by the neighboring jurisdiction.

Agency C was responding to a high-speed chase involving a motorcycle approaching the border of a neighboring city. Because units in the neighboring jurisdiction were monitoring Agency C's talk group, those units were able to initiate a roadblock and apprehend the suspect prior to being contacted. The use of the scan feature aided in the successful outcome of this incident.

As shown in the example, the use of the scan function results in decreased response times and more efficient use of resources, which may produce benefits for all agencies involved.

- **Regularly Monitor Land Use and Urban Development**. Increased land development can have a negative impact on communications coverage depending on the types of buildings constructed. For example, buildings may block radio signals

depending on their size. Moreover, the original trunked LMR system may have been designed to provide mobile radio coverage in an area that was undeveloped.

Furthermore, urban sprawl can negatively impact system coverage. The first signs of this impact usually come in the form of the inability of portable radios to operate within buildings. Agencies may want to consider participating in building permit application reviews as well as conducting radio coverage testing in new or existing buildings as a part of the fire or certificate of occupancy building inspection process. The erection of multistory structures will affect coverage and may impact the original system design; therefore, the local government may want to implement zoning or administrative processes that require the developer to bear the cost burden of improving in-building coverage.

An area within Agency G's jurisdiction was evolving from mainly grasslands to a dense housing subdivision. Because of this change, improved coverage would be needed to support calls for service in this area. By monitoring the situation, the radio manager was able to develop a plan in advance to ensure adequate system coverage for the future.

- **Understand the Permit, Zoning, and Building Codes for Tower Sites**. Some regions of the country have complicated codes for erecting communications towers. In some instances, work such as applying for the appropriate permits and site surveys may need to be completed months to years in advance to ensure that the tower(s) can be constructed. Obtaining the necessary permission could hinder trunked system development and operations if additional communications towers are required. System managers may also find it useful to work closely with knowledgeable zoning and building officials in their area to expedite the process. Additionally, system managers may need to consider federal environmental and historic preservation regulations regarding tower sites. These are discussed in the PSWN Program's *Special Assignment Technical Report—Siting of Communications Towers*. Officials should also monitor and evaluate urban development patterns as they progress in order to make informed decisions regarding system expansion and tower replacement.

- **Consider Infrastructure Sharing and Relationship Building with a Variety of Internal and External Agencies and Commercial Service Providers**. Several system managers stated that resource sharing resulted in cost and time savings.

One regional system manager developed a relationship with a federal department. The regional system manager and federal representative entered into an agreement in which regional system equipment was installed on three federal properties lease free, while federal equipment was installed on the regional system without cost. This cooperative effort allows the federal department to establish communication with local and state agencies during wild land fire incidents.

In addition, by developing relationships with commercial service providers, some system managers have been successful in collocating their equipment at a commercial tower site. Because the owning public safety agency does not bear all the costs for

the site, this arrangement saves time and money. Coordination with other governmental departments and commercial wireless carriers can produce economies of scale when these entities build towers or purchase land that could be used to support future system needs.

4.2 Operational Best Practices

This section describes the best practices associated with the operational environment. To help guide the reader, considerations are segmented in the following categories—talk group organization, system administration, interoperability, and training. Summarized in Table 4 are the operational best practices identified during the course of the data collection for this report. Also included here are "real world" examples (shown in "gray" text boxes) of operational best practices from several agencies across the Nation. Descriptions of each of the agencies (listed as agencies "A" – "L" to ensure anonymity) are detailed in Appendix C.

Table 4
Operational Best Practices

Consideration	Best Practices
Talk Group Organization	• Involve the user community in planning
	• Define a default fleet map
	• Develop a standardized template across domains
	• Regularly review fleet maps and talk group plans
System Administration	*System Planning*
	• Develop a disaster recovery plan
	• Inform dispatchers of system upgrades
	• Create a regional news group
	• Monitor system statistics
	Database Management
	• Track the distribution and maintenance of subscriber units
	System Maintenance
	• Perform routine system failure testing
	• Develop and implement a formal maintenance plan
Interoperability	• Implement special operations or coordination talk groups
	• Match unit numbers and zones when sharing subscriber IDs in a region
	• Consider transportable interoperability solutions to address commercial interference
Training	• Establish training teams
	• Survey users to identify systems concerns
	• Develop multiple training delivery formats
	• Employ visual aids

4.2.1 Talk Group Organization

The best practices for establishing talk groups, as identified during the course of this study, are shown in Table 5—

Table 5
Talk Group Organization Best Practices

Consideration	Best Practices
Talk Group Organization	• Involve the user community in planning
	• Define a default fleet map
	• Develop a standardized template across domains
	• Regularly review fleet maps and talk group plans

- **Involve the User Community in Planning**. The user community should be involved actively in fleet map development to ensure that various communication needs are fulfilled. Users will gain a better understanding of how communications occur on a trunked system and how interoperability can be achieved. Additionally, users will be more accepting of the system and the changes it may bring if they have been involved in the development of important system aspects that significantly affect their communications. System managers should coordinate user groups consisting of a communications representative(s) from each division or agency.

Agency F organizes three users groups (law enforcement, fire, and public works) to ensure that operationally effective fleet maps are developed. Because the user groups are heavily involved in talk group planning, communications officials believe that the users are more accepting of the new system despite some operational changes.

- **Define a Default Fleet Map**. In every step of a communications transmission, subscriber units and the central controller use IDs. The process of assigning IDs is called fleet mapping. An ID is a hexadecimal[2] number typically composed of the system ID, talk group ID, and the unit or individual ID. Fleet maps should be based on users' needs and missions, and not solely on the organization's structure. Radio managers may find it useful to define their default fleet map first before building a more detailed talk group plan. In the event of system failure, subscriber units will revert to the default fleet map for operations. From the default fleet map, which supports basic operations, radio managers can begin to build a robust operational fleetmap to support a variety of operating scenarios.

- **Develop a Standardized Fleet Map Template Across Domains**. A standardized template across domains may reduce radio reprogramming efforts, saving time and money. Additionally, if radios have a standard template, then ideally any user should be able to operate effectively from any radio on the system because the talk group

[2] A numbering system containing 16 sequential numbers as base units before adding a new position for the next number. The hexadecimal numbers use 0–9 and then use A–F.

order is standardized. In addition, template standardization streamlines future programming efforts.

- **Regularly Review Fleet Maps and Talk Group Plans**. Updating and revising fleet maps and talk group plans helps to ensure that the system is operating in the most efficient manner. A review should be performed annually or bi-annually depending on the system size and complexity. During the review, the system manager may analyze system statistics, large-scale personnel or staffing changes, and geographic considerations. A study of each of these components may reveal limited usage of certain talk groups or congestion of others. However, depending on the size of the system, an extensive radio reprogramming effort may be necessary. It is important to coordinate these efforts with jurisdictional neighbors if talk groups are shared across systems to achieve interoperability. Updating or changing the fleet map or talk groups for one jurisdiction may affect regional users by forcing those users to reprogram radios as well as to maintain the current level of interoperability.

4.2.2 System Administration

Outlined in Table 6 are the best practices identified for system administration. To guide the reader, the section is further segmented into system planning, database management, and system maintenance best practices.

Table 6
System Administration Best Practices

Consideration	Best Practices
System Administration	*System Planning*
	• Develop a disaster recovery plan
	• Inform dispatchers of system upgrades
	• Create a regional news group
	• Monitor system statistics
	Database Management
	• Track the distribution and maintenance of subscriber units
	System Maintenance
	• Perform routine system failure testing
	• Develop and implement a formal maintenance plan

➢ ***System Planning Best Practices***

- **Develop a Disaster Recovery Plan**. Because the ability to forecast potential disasters is limited, public safety agencies should develop and implement disaster recovery communications plans prior to system implementation. For example, natural disasters such as earthquakes or hurricanes are not predictable and pose a considerable threat to life and property. Therefore, public safety agencies should have a backup communications plan that would allow public safety officials to fulfill their responsibilities should the primary system go "offline". Specifically, agencies should not wait to develop a disaster recovery plan until after a new communications

system has been implemented because the lives of public safety officials and the public could be put at risk. Modern trunked radio systems offer unique opportunities to develop different system configuration pre-plans that can be implemented based on the type or location of the emergency event.

- **Inform Dispatchers of System Upgrades.** Dispatchers play a critical role in public safety communications and serve as an interface between the public safety community and the public itself. Therefore, dispatchers should be equipped with the most current system information, which includes being notified of system upgrades or modifications. System upgrades or modifications could alter the routing of calls. For example, changes to the design of the system's talk group plan could alter talk group numbering causing talk groups to be patched incorrectly. Dispatchers should receive timely e-mail or fax notifications of system changes. Like other system users, dispatchers should be consulted regarding any changes involving dispatcher console positions and radio system access capabilities. System managers should consider and facilitate adequate testing and evaluation of console configurations, seeking appropriate feedback if possible. These activities should occur in a testing environment prior to implementation in the live environment.

- **Create a Regional News Group.** Public safety agencies should stay abreast of technological advancements, Federal Communications Commission (FCC) policy and rulemakings, as well as industry and operational trends. A simple way to stay current with technological trends is to monitor industry-related magazines and Web sites. Agencies should monitor standards bodies such as the Telecommunications Industry Association (TIA), Electronic Industries Alliance (EIA), and American National Standards Institute to remain familiar with the most current telecommunications standards established by these organizations. In addition, public safety-related communications information could be found by participating routinely in or monitoring developments within the International Association of Fire Chiefs or International Association of Chiefs of Police. To obtain regular updates and maximize the use of available resources, agencies should coordinate regionally to design news groups. News groups enable public safety personnel to gain access to the latest industry-related information by e-mail, fax, or other modes of dissemination. Typically, one or several individuals within a region collect the information distributed through news groups.

One region appoints an individual to collect recent developments in the industry and communicate the information via a news group, which is supported by a popular Web search engine. The functionality of this news group enables individuals in a region to receive regular updates via e-mail and become educated regarding industry and regional developments.

- **Monitor System Statistics.** Using network management tools, public safety agencies should continually monitor and analyze system statistics to gauge and improve the trunked radio system's quality of service. Often, a radio system may appear to operate efficiently under normal conditions, but certain system features or operational methods may produce bottlenecks that could hinder performance during a challenging

situation. To identify these bottlenecks, system administrators should generate system statistics regularly. The size of an agency and volume of communications may dictate the need for system statistics. It is also important to note that system statistics can help justify the need to upgrade or purchase a new system by reflecting the load, channel congestion, and number of busy tones. By analyzing the system's performance regularly, system managers can help ensure the availability of service to its customers and validate the need for system enhancements.

- ***Database Management Best Practices***

  - **Track the Distribution and Maintenance of Subscriber Units.** By tracking the distribution and maintenance of subscriber units, public safety agencies can gain a historical perspective on past efforts and current work related to those units. A historical perspective allows system maintenance personnel to troubleshoot problems with subscriber units by analyzing the service record of a particular unit. To that end, a comprehensive database should be developed to track subscriber units throughout their life cycle.

To manage its large population of users, Agency J developed a database tool for subscriber units that tracks the date it was added to the system, where the unit was assigned, and past reprogramming efforts. Further, when radios need reprogramming, the database enables system managers to track those units that have and have not been reprogrammed. As a result, units that have not been reprogrammed are located easily using the database, and maintenance modifications can be made.

- ***System Maintenance Best Practices***

  - **Perform Routine System Failure Testing.** By performing routine system failure tests, public safety agencies can analyze system functionality and prepare personnel for potential system failures. As shown in Appendix E, once a trunked radio system fails, it enters either site trunking[3] or fault tolerant mode[4] depending on the circumstances. Testing several times per month enables an agency to verify normal, site trunking, and fault tolerant modes are operating correctly and ensure its personnel are accustomed to operating in each mode. In addition, system managers can analyze system performance during failure and reconfigure the system as necessary. Testing also prepares technicians, dispatchers, and field personnel for system failure by exercising their ability to function normally and to use equipment properly under such conditions. Specifically, field personnel must become familiar with the audible tone emitted from mobile and portable subscriber units when operating in fault tolerant mode. Often, these tones can be extremely loud and distracting to the user. Therefore, system administrators should test the volume level of the tone in subscriber equipment prior to distribution.

[3] Site trunking occurs when a transmitter loses the ability to communicate with the zone controller. Radios can only communicate with other radios affiliated with that site.
[4] Fault tolerant mode occurs when the transmitter site with which a radio is affiliated fails and cannot perform trunking, causing the radio to switch automatically to a predetermined frequency.

To ensure all personnel take part in system failure tests, tests should be performed during each shift and occasionally without notice. Typically, agencies inform their personnel when system failure tests are planned. However, agencies should perform ad hoc failure tests to assess the ability of personnel to handle unplanned system failures.

- **Develop and Implement a Formal Maintenance Plan.** A formal maintenance plan should be implemented to facilitate the inspection and maintenance of software, equipment, and system infrastructure. For example, common trunked system failures, such as alarm and backup battery failures, can be mitigated through periodic tests and replacements. To facilitate this effort, an established maintenance plan that provides a schedule for conducting routine and preventative maintenance would prove valuable for public safety agencies. Maintenance plans should include a detailed description of the tasks to be performed and the resources required to complete them. Guidance should be provided detailing these tasks to ensure maintenance is performed appropriately. Moreover, trunked systems are more technically complex than conventional systems, highlighting the need for an established approach to trunked system maintenance. Appropriate maintenance provision tracking can help to identify problem areas and needs for specific attention to components that fail repetitively. The collection of such information assists with the justification for continuing maintenance funding and future component or infrastructure replacements.

Agency F exercises backup generators once per week. Furthermore, this agency tests the generators under load (i.e., during rush hour or under normal operating conditions) for substantial portions of time to analyze the ability to function throughout peak communications periods. As a result, Agency F is aware of power outputs and can ensure system availability under the most demanding environments.

In addition to system-related tasks, formal maintenance plans may include monitoring the physical environment of the system. Monitoring the physical environment includes testing alarms, telephone lines, and the security of communications sites.

4.2.3 Interoperability

Best practices for interoperability are summarized in Table 7.

Table 7
Interoperability Best Practices

Consideration	Best Practices
Interoperability	• Implement special operations or coordination talk groups
	• Match unit numbers and zones when sharing subscriber IDs in a region
	• Consider transportable interoperability solutions to address commercial interference

- **Implement Special Operations or Coordination Talk Groups**. Special operations or coordination talk groups are an effective means to achieving interoperability for preplanned events and emergency operations. Typically, these talk groups are used for a task force operation or for a special event such as a parade. Use of talk groups can be coordinated through a system manager by written request with adequate time to prepare. During the event, special operations talk groups are typically assigned across all disciplines.

- **Match Unit Numbers and Zones When Sharing Subscriber IDs**. Coordinating zones and subscriber IDs is a viable interoperability solution for agencies in the same region that operate on technologically similar systems (i.e., systems manufactured by the same vendors and that use the same frequency band). Coordinating subscriber IDs and zones may help to improve the management of subscriber IDs while enhancing interoperability. In some regions, various jurisdictions share and swap subscriber IDs to achieve interoperability. This allows a subscriber unit to operate on its home system and other systems in the region. To facilitate interoperability and the management of subscriber IDs, each system has a zone number, and the beginning of the subscriber IDs corresponds to that zone. For example, all users in Zone 1 have IDs that begin in the 100s while users in Zone 3 have IDs that always begin in the 300s.

- **Consider Transportable Communications Solutions to Address Commercial Interference.** Public safety agencies can use a transportable solution to address commercial interference or interoperability shortfalls. Often, this transportable solution comes in the form a portable repeater or receiver system that can be used to allow better communications between personnel using low-powered portable units. This solution could be effective in areas where the volume of commercial telecommunications traffic results in a high level of interference. Commercial interference can hinder the ability of public safety agencies to communicate and frequently results in busy tones or the inability for the user to acquire a channel. Moreover, the effect of interference is magnified when considered in the context of major events where thousands of people gather within a small geographic area or venue such as a stadium or amphitheater. Therefore, to ensure an acceptable quality of service (i.e., ability to acquire a channel in a timely manner), public safety agencies should seek solutions that can be leveraged to overcome such barriers to efficient communications.

One such solution used by Agency E involves using a transportable communications unit that can be deployed on-scene at major events. Essentially, this transportable unit serves as an additional repeater on the system and reduces the range between the existing repeater and subscriber units; thereby, increasing coverage reliability. More importantly, Agency E incident commanders are aware of the existence of the transportable communications unit and understand how its capabilities can be leveraged to improve interoperability across a broad range of potential incidents.

Not only can a transportable communications unit be used to address commercial interference, it can also fulfill a number of other objectives. The mobile nature of this solution works to provide interoperability among first responders, supplement or extend the coverage of fixed infrastructure systems, and enhance local, state, and federal interoperability during emergency situations and special events. One such solution (identified in PSWN Program documents as the Transportable Public Safety Radio Interoperability Unit) uses an audio cross-connect switch to link public safety radio systems using different frequency bands.

A transportable solution can be configured in a variety of ways to address both commercial interference and interoperability constraints. As such, agency objectives and requirements should drive the design of a transportable solution.

4.2.4 Training

Best practices associated with training issues are summarized in Table 8.

Table 8
Training Best Practices

Consideration	Best Practices
Training	• Establish training teams
	• Survey users to identify systems concerns
	• Develop multiple training delivery formats
	• Employ visual aids

- **Establish Training Teams**. A dedicated, skilled training team is an ideal training resource for developing a highly knowledgeable workforce. A training team can be selected from the current pool of field users in each public safety discipline served by the system including dispatchers and radio technicians. This diverse team can lend instant credibility to a training program and may further encourage user "buy-in." Once a team is formed, certified according to designated state and local regulations, and trained through the appropriate technical sources, trainers can focus on developing user-specific LMR introductory, continuing, and remedial training sessions. For system improvements or modifications, trainers can offer detailed in-service or training updates as needed. Trainers should be involved in trial and/or testing exercises of new features or significant configuration changes.

Agency H has established a full-time training team capable of responding to various demands of a large user population. Each member of the training team must meet a rigorous in-house certification program that incorporates, lesson planning, training aid and documentation development, presentation skills, technical knowledge, and operational considerations. With the use of dedicated personnel, Agency H is able to maintain a staff of knowledgeable and professional LMR trainers supporting the varied user population.

- **Survey Users to Identify System Concerns**. Issuing user surveys can help uncover a variety of concerns. Due to their limited LMR technology background, many users

may be unable to communicate concerns effectively regarding usage or performance of system features, or training limitations. By developing a targeted survey encompassing a broad range of operational aspects, trainers may be able to pinpoint training shortfalls quickly. In addition, survey results may also help communications officials uncover system performance issues.

- **Develop Multiple Training Delivery Formats.** The nature of the public safety environment requires a flexible and varied training format. As such, an introduction to LMR communications would be a great benefit for the new user. Further, refresher training should be provided for veteran users to stay informed of system modifications, operational changes, and seasonal events. Beyond instructional classroom and traditional on-the-job training, agencies can implement a variety of formats for focused training modules, including roll-call presentations, e-mail notifications, and newsletter updates. System overviews and training of lesser-used system features and functionality should be provided, at a minimum, during annual in-service training courses.

Agency E distributes ad-hoc newsletters to address communications concerns and associated seasonal events. In preparation for natural disasters, users receive a newsletter describing the radio communications failure plan (i.e., fallback plan), operational guidelines, and other related procedures. This format allows the agency to present valuable and timely information without requiring a formal training situation.

- **Employ Visual Aids.** The power of an image is unsurpassed for conveying volumes of information. Several visual aid materials are appropriate for radio communications training beyond the traditional use of slides and overhead transparencies. For introducing equipment, increasing familiarity with features, and presenting new procedures, videos and photographs serve as enhanced training tools. The use of actual user equipment during training sessions to demonstrate methods or functions interactively can significantly enhance training opportunities. Furthermore, the ability of users to demonstrate problems or difficulties interactively on the actual equipment provides an additional avenue for feedback and instruction. Also, system coverage area maps can be used to identify problem coverage areas for technical investigations and potential corrections.

Several agencies noted that they used photographs and videos for radio communications training. Agency B presents the region's radio sites in pictures. This training aid provides the geographic location in conjunction with a visual display of the radio equipment, thereby enhancing the learning opportunity. Videos offer a unique opportunity for an agency to capture subscriber equipment and the associated communications procedures in a simulated or live-action sequence. Agency H widely distributes videos to all of its user segments identifying equipment and general operating procedures, as well as basic maintenance tasks. These agencies consider photographs and videos as a value-added resource appreciated by users and trainers alike.

4.3 Political Best Practices

As summarized in Table 9, this section details best practices associated with the political arena. Although the focus of this report is operational activities, the majority of interview subjects noted the impact the political arena has on public safety communications. Also included here are "real world" examples of political best practices from several agencies across the Nation. Descriptions of each of the agencies (listed as agencies "A" – "L" to ensure anonymity) are detailed in Appendix C.

Table 9
Political Best Practices

Consideration	Best Practices
Political	• Participate in working groups
	• Share resources
	• Garner stakeholder and user acceptance

- **Participate in Working Groups.** Working groups provide a forum for members to participate in discussions centering on shared challenges. To provide a common focus, membership is usually limited to organizations with similar technology interests or operational concerns, or a similar geographic region. For public safety agencies, internal working groups composed of system users can explore and develop strategies actively regarding numerous issues, including key stakeholder education, user training, interoperability, and operational recommendations. User groups consist of a variety of levels of public safety officials, including field personnel, agency supervisors, and system management personnel. By organizing a group of public safety officials with varying duties and responsibilities to discuss communications issues, the system manager can collect wide-ranging opinions related to the service of the communications system. The resulting dialog enables the system manager to resolve many issues related to user error or problems in the field, and in turn, tailor the system to the individual needs of the user agencies.

  Regional working groups may offer a broader perspective on concerns similar to those managed by internal working groups. Regional working group membership generally encompasses the public safety community within a large geographic region. These groups are uniquely positioned to stress close cooperation and coordination among participants regarding high-impact alternatives such as equipment purchases, system enhancements, interoperability methods, and public safety response.

Composed of several ranking members, field users, and radio technicians, Agency C's formal internal user's group serves as a sounding board for technical and operational concerns and recommendations. For example, field users noted a specific event in which responders were unable to hear each other. The radio technicians were able to isolate this incident on prerecorded tape and determine, in conjunction with the responders, that the issue was not coverage but user error. This group has successfully identified, assessed, and remedied operational concerns through an effective group forum. Further, this has yielded an unprecedented partnership within this agency among communications officials and field users, bridging the gap between problem identification and solution**.**

- **Share Resources.** Public safety agencies can share resources to minimize costs and maximize efficiency and interoperability. Resource sharing can take a number of forms, including spectrum sharing and combined use of infrastructure, each of which may facilitate interoperability. In addition, operational complexities are reduced because agencies operate on a common platform, eliminating common barriers to interoperability such as disparate frequency bands and incompatible technologies. Resource sharing, however, requires a high level of coordination that is often achieved through regional or statewide work groups.

Agency H has partnered with other agencies in its region to implement a shared, regional communications network. These agencies share system resources including spectrum and infrastructure, as well as costs associated with operations and maintenance. Cost savings have enabled the region to acquire advanced technologies such as Global Positioning System and automatic vehicle location. In addition, to promote interoperability, the agencies designed the system to allow other local, state, and federal users access to the system. This regional partnership is a prime example of agencies achieving interoperability while increasing coverage and implementing advanced technologies.

- **Garner Stakeholder and User Acceptance**. Communications officials must garner support from numerous sources to manage a LMR system and to plan for future improvements. A continuing, open dialog between key stakeholders, field users, and radio technicians is necessary to identify and resolve issue areas, plan for system enhancements and improved interoperability opportunities, and participate in regional solutions.

During the initial planning stages of Agency G's 800 megahertz trunked system, communication officials were able to gain the support of several key senior leaders within the public safety community through a grass roots campaign. Building on this, senior leaders and technical representatives established a comprehensive outreach effort that consisted of informal discussions with small groups of field users, public safety union officials, government leaders, and other interested parties. The outreach efforts were finally expanded to encompass neighboring jurisdictions and federal users. According to communications officials, this systematic approach to garnering the necessary support propelled the development of the system, a timely implementation, and ultimately, user acceptance.

5. LESSONS LEARNED ASSESSMENT

This section details lessons learned from various public safety agencies participating in this study. The featured lessons describe practices that helped to avert undesirable or ineffective overall management of trunked systems while enhancing interoperability and optimizing associated operational practices. The lessons learned are grouped by operational and technical considerations and are summarized in Table 10. Also included here are "real world" examples (shown in "gray" text boxes) of lessons learned from several agencies across the Nation. Descriptions of each of the agencies (listed as agencies "A" – "L" to ensure anonymity) are detailed in Appendix C.

Table 10
Lessons Learned

Consideration	Lessons Learned
Technical	• Trunking protocols do not have a noticeable impact on operations
	• Security Features are not widely implemented
Operational	• System documentation should be developed to facilitate transfer of knowledge
	• Assignment of subscriber IDs should be managed centrally
	• Alternative connectivity options should be investigated when implementing console-to-console patches
	• Implications of using an airborne platform for interoperability should be considered
	• Subscriber unit capacity should be considered when exchanging fleet maps as an interoperability solution
	• Generic training programs may be insufficient

As summarized in Table 10, the following technical lessons learned were noted—

- **Trunking Protocols Do Not Have a Noticeable Impact on Operations**. Based on data collected for this study, trunking protocols do not affect communications effectiveness. The protocol (i.e., message or transmission) that should be used when implementing a trunked system is a highly debated topic in the LMR industry. However, most system managers in this study had little knowledge of how the protocol affected operations and in some instances did not know which protocol had been implemented on their system.

- **Security Features Are Not Widely Implemented**. Although many systems throughout the state and local public safety communities are equipped with security features, in practice, these features are not widely used. In most cases, state and local public safety agencies do not require encryption for day-to-day operations. Typically, users such as narcotics or internal affairs officers most often implement encryption. Because the use of encryption is uncommon for the majority of users among state and local agencies, a user's ability to apply the encryption feature, when necessary, often lessens over time. For system managers, encryption key management can be logistically challenging due to the need to physically "touch" every subscriber unit to rekey it. The capability to accomplish over-the-air rekeying (OTAR), however, is

easing the burden associated with the need to physically rekey an entire fleet of user radios. OTAR enables automatic key distribution and permits efficient updating of encryption keys for field users.

As summarized in Table 10, the following operational lessons learned were noted—

- **System Documentation Should Be Developed to Facilitate the Transfer of Knowledge**. Communications system documentation is critical to the transfer of knowledge as personnel are reassigned, retire, or move on to other fields or organizations. The primary function of LMR system documentation is to record infrastructure, equipment, and talk group design considerations and functionality. In addition, documentation serves as a tracking mechanism for system modifications and enhancements, as well as the intellectual capital of system managers. By recording system-related information, agencies can facilitate the transfer of knowledge between system managers and other individuals involved in the system management function. If not properly documented, valuable information could be lost. Agencies acquiring new systems should require comprehensive "as-built" documentation, including technical drawings and diagrams documenting the system as delivered from the supplying vendor. The documentation should cover the entire infrastructure and all related sub-systems. The documentation should be provided in an industry-recognized and updateable electronic form so that system changes can be recorded.

One agency originally designed its trunked system to be interoperable with others in the region via regional interoperability channels. However, at that time, there was little need for interoperability, and the channels went unused. After the system manager retired, public safety missions expanded and the need for interoperability became significant. Although the functionality was available in the system, the succeeding system manager was unaware of it due to a lack of documentation.

The public safety community should capitalize on this lesson learned and understand that documentation is essential. If the need for documentation is disregarded, the affect could be regionwide, resulting in poor interoperability.

- **The Assignment of Subscriber IDs Should Be Managed Centrally**. Because organizations must manage many subscriber IDs, a mechanism to facilitate the assignment of IDs should be developed. In some regions, IDs are shared to permit interoperability with other trunked systems in a region. Subscriber IDs are generally allocated in blocks of hundreds or even thousands. To ensure duplicate subscriber IDs are not assigned, system managers should develop or acquire a mechanism to facilitate this process. Spreadsheets or simple database applications can fulfill this requirement effectively. Such tools should be designed to store several key characteristics, including the hexadecimal subscriber ID number, the assigned alias, the agency to which the ID was assigned, and the date assigned. By collecting this information, system managers can track distributed IDs, thereby avoiding the assignment of duplicate IDs. If IDs are not properly managed, agencies may find it

difficult to identify the user, particularly in instances when the emergency button is used.

Agency B, a participant in a regional sharing arrangement, had no mechanism in place to track IDs. As a result, ID assignments were not recorded, resulting in a lack of knowledge regarding which IDs were assigned and when. Note that neglecting to track the assignment of subscriber IDs can have a regionwide effect because some agencies share IDs for interoperability purposes.

- **Alternative Connectivity Options Should Be Investigated When Implementing Console-to-Console Patches.** Many agencies use the console-to-console patching solution to achieve interoperability. Console-to-console patching refers to the use of central dispatch consoles for an audio interconnect. Typically, consoles are connected in one of three ways—

  – Public switched telephone network (PSTN)
  – Dedicated leased line
  – Dedicated microwave or fiber link.

  The use of console-to-console patching introduces latency in the form of dispatcher intervention and setup time and is also dependent on the geographic separation of the consoles being connected. However, setup time and dispatcher intervention may not be a factor if the consoles are connected permanently. From an operational perspective, latency can affect the ability of public safety officials to communicate in real-time and it can reduce operational efficiency. Patch latency also increases transmission time per message, potentially limiting system capacity during the patch in trunked systems using the transmission protocol. To reduce the effect of latency, agencies should consider using microwave connections or leased lines rather than the PSTN. Transmission speeds over microwave connections are inherently faster than PSTN connections and minimize delays because dispatcher intervention is not required. However, it is important to note that FCC licenses for microwave bands may slow implementation, require legal support, and increase costs. In addition, the initial investment to acquire microwave equipment may be significant. The incorporation of permanent patches using PSTN or dedicated lease circuits also requires backup and restoration planning in the event the patch is disabled. Appropriate facilities to continue critical operations should be predefined, and priority restoration services agreed upon with commercial providers.

- **The Implications of Using an Airborne Platform for Interoperability Should Be Considered.** Public safety agencies achieve interoperability in a variety of ways. Often, agencies must develop unique solutions to realize or maintain communications with one another. Geographic location and jurisdictional boundaries are two of the primary drivers of unique interoperability solutions. Regardless of how useful these solutions may seem, agencies should consider the implications of the solution on the operational effectiveness of the organizations involved. For example, when Agency G advances beyond its radio system's coverage area, it uses a helicopter to relay messages from one jurisdiction's units to another and to communicate back to the

dispatch center. While this solution is unique and may appear valuable on the surface, agencies must consider the drawbacks of such an arrangement. First, personnel trained to operate a helicopter have a demanding responsibility to maintain an aircraft and may not be best positioned to serve as the intermediary in an emergency. Second, the inherent distortion of message content when routed between a number of personnel may hinder the response. Finally, the use of an intermediary introduces significant delay that could result in putting lives and property at risk. Nevertheless, agencies must evaluate the advantages and disadvantages of each potential interoperability solution and select the solution with the least negative impact on organizational effectiveness.

- **Subscriber Unit Capacity Should Be Considered When Exchanging Fleet Maps as an Interoperability Solution**. Often, when multiple communications systems exist in a region and developing a shared infrastructure is not a potential solution, public safety agencies look to exchange fleet maps to achieve interoperability. Because each agency's talk groups are programmed into one another's subscriber units, each agency has the ability to communicate on the other agency's system, irrespective of home system coverage. Therefore, providing that fleet maps have been exchanged regionally, it can be assumed that regional interoperability exists between these agencies. However, the number of talk groups programmed into the subscriber units could be relatively high and the potential exists for the number to increase rapidly as additional agencies participate in the sharing arrangement. Although this solution may work well when implemented across a limited number of small to medium sized agencies, the capacity of subscriber units must be considered. In some cases, it may be prudent to share only a subset of specific talk groups and agency IDs with neighboring agencies so as to not overwhelm the subscriber unit capacity. Furthermore, a heavily programmed subscriber unit more readily contributes to operator errors due to the vast numbers of systems, talk groups, or modes programmed into the unit.

To achieve regional interoperability, Agency H considered exchanging fleet maps with other agencies in the region. However, this solution was deemed inadequate because several agencies could not be included due to limited subscriber unit capacity. As the number of agencies or number of fleet maps exchanged increases, available subscriber unit capacity decreases. Therefore, agencies should seek to plan interoperability solutions regionally. In this way, they will be less likely to preclude interoperability with other agencies due to equipment constraints.

- **Generic Training Programs May Be Insufficient.** Nonspecific training programs, generally delivered by vendors, may prove inadequate for field users and radio technicians. Generic training will likely refer to basic user operations and equipment features with no reference to customization that reflects agency-specific jargon, location addresses, protocols, and missions. Due to the inherent complexity of radio communications and equipment operations, users typically benefit from a more tailored approach. Vendors should be required contractually to provide levels of training targeted to specific user groups (e.g., dispatchers, police officers/firefighters,

technicians, system managers). These targeted training activities should be developed to be consistent with the system's capabilities and configuration.

6. CONSIDERATIONS AND CONCLUSIONS

Based on the data collection and analysis effort, the PSWN Program identified several significant considerations and conclusions, which may prove useful to public safety agencies nationwide. These considerations and conclusions are not directly addressed in the Best Practices and Lessons Learned sections of this report. The concepts detailed in these additional considerations are critical, as they each can have significant impact on the operational effectiveness of trunked radio systems, and by extension on interoperability. In light of this, each consideration and conclusion should be reviewed and applied throughout the system planning process, and in particular, as agencies migrate to new radio systems and technologies. Note that as agencies begin to apply these concepts, additional planning, development, and implementation resources and activities may be required. The considerations and conclusions are shown in Table 11.

Table 11
Considerations and Conclusions

Considerations
• Consider the application of over-the-air programming
• Consider the implications of Project 25
Conclusions
• The potential impact on internal and external environments should be considered when selecting an interoperability solution
• Subscriber ID sharing should be managed properly and coordinated regionally
• The scope and reach of an organization should drive fleetmap development

As summarized in Table 11, the following should be considered—

- **Consider the Application of Over-the-Air-Programming.** Recent advances in technology have introduced over-the-air-programming (OTAP) as a viable alternative for the public safety community. OTAP permits alteration of a subscriber unit's programs via remote commands while that unit is deployed in the field. Essentially, OTAP replaces the cables needed to interface with a computer with radio waves, permitting reprogramming anywhere within the system's coverage area. In addition, multiple radios can be reprogrammed with a single transmission, reducing the time and personnel resources traditionally required to accomplish fleet-wide reprogramming efforts. Although OTAP presents many operational advantages, it also has several limitations. First, transmitting system parameters over the air introduces security concerns, such as eavesdropping and spoofing. Secondly, because the introduction of the concept of OTAP is a relatively recent one in the public safety community, the costs for acquiring radios and equipment capable of OTAP may be high.

- **Consider the Implication of APCO Project 25 (P25)**. Rapid development of wireless technologies, incompatible technologies, and the lack of vendor competition motivated public safety personnel to participate in the development of a suite of open

standards for trunking. Commonly referred to as P25 (although it has now evolved into the TIA/EIA 102 suite of standards), this standard development effort focuses on improving interoperability among public safety radio systems and introducing market competition to the lifecycle of radio equipment. Because it may be necessary for public safety agencies to replace their equipment several times during the system lifecycle, the need for open standards is magnified. Without open standards, public safety agencies would be locked into purchasing equipment from the same manufacturer, in turn, reducing price competition and the opportunity for competitive procurements in the marketplace.

Public safety agencies can and should chose an LMR technology that best fits their operational needs now and into the future. Extensive and deliberate examination of the purchasing agency's needs as well as the needs and future system development efforts of neighboring agencies must be taken into account, and interoperability must be a primary consideration. The selection of a proprietary or standards-based (i.e., P25) technology solution is a decision that each user agency must make and should not be contemplated in a vacuum. Operational needs and interactions with neighboring agencies, existing systems, migration plans, and funding opportunities must all be weighed in the overall decision process. Standards-based systems also offer a planned migration path to the future generations of technology systems. The selection of a standards-based technology, while not perfect, will provide a more open technical environment that will encourage more manufacturers' participation as more systems are deployed. Appendix G contains a more in depth discussion of P25.

As summarized in Table 11, the following conclusions emerged from the data collection and analysis effort—

- **The Potential Impact on Internal and External Environments Should Be Considered When Selecting an Interoperability Solution.** Interoperability should not be planned or established without considering its effect on the internal and external public safety environment. Internally, agencies should seek to build consensus among all agencies and jurisdictions that may be impacted before selecting an interoperability solution. Externally, coordination should occur locally and regionally with neighboring jurisdictions to plan for and establish interoperable communications during an incident requiring mutual aid or task force assistance, as well as during large-scale disasters. In addition to internal and external coordination, active and constant dialog among public safety officials and politicians from all levels of government is needed to share information and build on effective solutions for fostering interoperability.

  While it is important to address current interoperability needs, public safety officials should also consider the future interoperability requirements of the region when planning for a new system or developing a long-term interoperability plan. To achieve this objective, agencies should coordinate large-scale changes with those agencies internal and external to the organization. If an agency disregards the needs of others in the region and implements a new system or solution that meets its

requirements exclusively, the result could hinder interoperability for many years, due to the usual 10-year system lifecycle of such a system. Conversely, agencies in a region that are planning new, simultaneous system implementations should look to pool their resources to develop a shared system that is mutually beneficial to each agency involved.

Formal planning committees or user groups are ideal for addressing strategic as well as tactical interoperability issues. By addressing interoperability issues, agencies can determine the technical means for achieving interoperability and establish joint exercises to prepare for emergencies.

- **Subscriber ID Sharing Should Be Managed Properly and Coordinated Regionally**. In some regions, sharing subscriber IDs as part of an interoperability solution has been effective. Different sharing methods can be used, including "wholesale sharing" or "limited sharing". Wholesale sharing occurs when an agency provides all or a majority of the user population's subscriber IDs to regional agencies. Conversely, participating agencies can elect to establish a limited sharing arrangement in which they exchange the common subscriber IDs associated with each domain.

  To facilitate the assignment of subscriber IDs regionally, a central point of contact is needed to maintain and administer the IDs. As stated above, a central repository for collecting and storing subscriber IDs would be required. In addition, all subscriber IDs allocated for regional interoperability would be coordinated through this contact. While a central point of contact seems realistic, the political implications of such an arrangement must be considered. First, determining what agency will serve as the central point of contact for a region may be complex due to control issues and security concerns. Secondly, due to the nature of public safety operations, it may be difficult to persuade the agencies' system managers to coordinate with one another. However, the value proposition presented by such an arrangement outweighs the alternatives. For example, if subscriber IDs are managed properly, the need for duplicate reprogramming efforts is minimized, thereby reducing costs and freeing up personnel to fulfill other obligations. Agencies can leverage existing relationships in the region to build consensus for an arrangement that will benefit each participant.

- **The Scope and Reach of an Organization Should Drive Fleetmap Development. T**he user community should be involved in the planning process for trunked radio systems, and as such, fleet maps and system access should be based on user need and mission. In several instances researched in this study, system access was based on the political power an agency yielded within a jurisdiction or region. Political clout should not bear weight in this arena as all public safety missions are equally important and should be given an equal voice in the system planning process.

  To that end, communication is a key aspect of understanding the needs and objectives of various agencies within a jurisdiction or region when planning a new trunked system or interoperability solution. Communication among agencies at all levels of

government enables agencies to understand one another's requirements. Further, communication can break down barriers, manifested as turf issues and power struggles, that heretofore have been difficult to overcome. As agencies engage one another, it is important to bear in mind the responsibility and mission of their respective organizations, and to consider the ramifications of their choices on the citizens they serve.

APPENDIX A—TRUNKING OVERVIEW

APPENDIX A—TRUNKING OVERVIEW

This appendix presents a tutorial on the fundamentals of trunking as it applies to the land mobile radio (LMR) environment. Specifically, it provides a technical description of trunking, introduces talk groups, and discusses the advantages and disadvantages of trunked radio systems.

Because spectrum is a limited resource and can be costly to obtain, manufacturers developed trunking systems to optimize the use of available licensed channels. In general terms, trunking is the commonly accepted term for electronically controlled sharing of a relatively small number of communications channels among a relatively large number of users. In contrast to a conventional system in which users communicate over a dedicated channel, a trunked system uses a computer-driven controller to dynamically assign a channel to a user or group of users on a call-by-call basis. When a user presses the push-to-talk button, the system controller checks the ID of the talk group with which the radio user wants to communicate, checks for a vacant channel, and sends channel assignment instructions on the control channel to all of the radio units presently selected for that talk group. After a channel is assigned, the assigned users have private use of that channel. If no channels are free, the request is sent to a queue where it remains until a channel is available. Once the conversation is complete, the channel is returned to the pool of channels where it is available to other users.

This process takes advantage of the fact that not all channels are used simultaneously, thus employing available bandwidth more efficiently than conventional technology. For example, on a 10-channel conventional system, approximately 350–500 users can be served, whereas those 10 channels on a trunked system could serve roughly 1,000–1,500 users. Additionally, the assignment of channels in a trunked system is completely transparent to the user. Figure A-1 illustrates an example of how a typical trunked radio system may allocate channels.

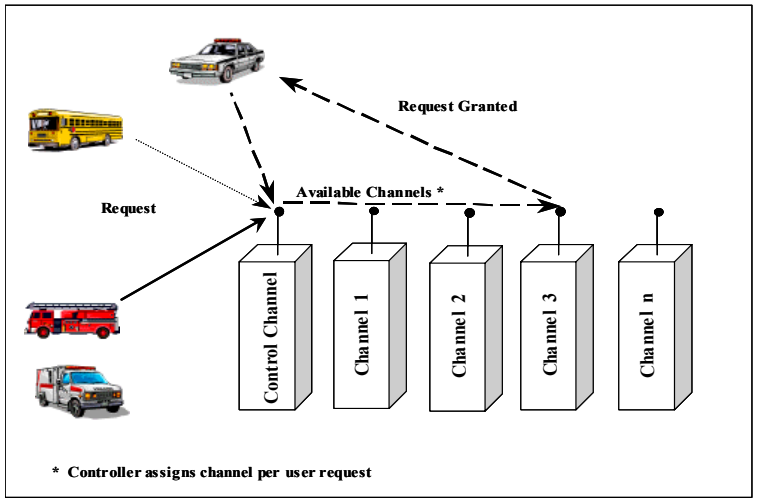


Figure A-1
Example of Channel Allocation in a Trunked Radio System

The primary difference between conventional and trunking technology is that a trunked system allows a group of users to share a set of available channels. These groups are commonly referred to as talk groups. A talk group is a preprogrammed, predetermined basic organizational group of LMR users. In a trunked system, each subscriber unit has a unique address that corresponds to a talk group. Users on a trunked system have the ability to switch between talk groups by physically turning the knob on their subscriber unit to a different number. Typically, users that have similar operational, functional, and technical requirements are divided into fleets. For instance, law enforcement, fire, and emergency medical services personnel are generally organized into a common fleet and then sub-divided into functional talk groups. As stated in the Public Safety Wireless Network Program's *How2 Guide for Establishing and Managing Talk Groups*, extensive planning and organizing is required to develop an effective talk group plan. If designed and implemented properly, an effective talk group plan will enhance existing system capabilities and provide flexibility over the long term.

- ***Advantages and Disadvantages to Trunking***

As public safety agencies implement new LMR systems, trunking is emerging as the preferred system technology. Driving its popularity are the numerous benefits that can be realized using trunked systems. The creation of new talk groups or adding new members to an existing talk group can be done in real time, allowing the formation of talk groups across organizational lines on an as-needed basis, thereby improving interoperability. In addition, trunked systems provide disciplined access to channels, which prevents users from creating interference with one another. Other advantages include increased user privacy, system scalability, and access to state-of-the-art features such as automatic unit ID, emergency alerting, talk group scanning, over-the-air dynamic regrouping, call prioritization, and telephone interconnect. Generally, public safety agencies request that these features and functionality be included in their LMR systems.

Although trunking presents many advantages, it may not always be the ideal solution for public safety agencies for a number of reasons. First, trunked systems are usually more expensive compared with conventional systems deployments. Lack of available funding is one of the primary obstacles for public safety agencies to overcome, making it difficult for them to afford new technology. Second, trunked LMR systems are not standardized across vendors, resulting in a number of proprietary technologies. Consequently, agencies using disparate trunked systems are unable to interoperate without implementing a solution to interconnect the systems. Possible solutions agencies could implement to facilitate interoperability are a console-to-console patch to interconnect the consoles of the systems using the public switched telephone network (PSTN), a dedicated leased line, or a dedicated microwave or fiber optic link. Third, a limited number of equipment manufacturers offer trunking technology. Summarized in Table A-1 are the major advantages and disadvantages of trunked systems.

Table A-1
Advantages and Disadvantages of Trunked Radio

Trunked Radio	
Advantages	**Disadvantages**
• Proven technology • Efficient use of frequencies • System redundancy and fault tolerance • Talk groups/channelization • State-of-the-art features • Adoption by larger agencies and regional systems • Service to more radios per channel • Wide coverage area through interconnection with PSTN and other trunked systems • Faster system access • Flexibility to expand • Reduced call retries through queuing call delay and call collision prevention • Reduced interference	• Higher cost • Technical complexity • Need to purchase new equipment • Potentially proprietary system • Need for more technically sophisticated maintenance • Limited number of manufacturers that offer trunking

Despite its disadvantages, trunking remains the preferred technology for public safety agencies because of its ability to enhance interoperability and improve spectral efficiency. Because of its dynamic channel usage, a trunked radio system provides the user with reliable, efficient access to channels during emergencies, as well as state-of-the-art features to ensure that calls are received. Often, agencies have no choice but to adopt trunking technology because of the limited quantity of spectrum resources available to public safety agencies. As a consequence an increasing number of public safety agencies are implementing trunking technology as they replace their existing systems.

APPENDIX B—DATA COLLECTION MATERIALS

Interviewer:_____
Date/time: _____

APPENDIX B—DATA COLLECTION MATERIALS

I. Contact/Demographic Information

1. Please provide the following information.

Name	Position and Division	Agency Name and Mailing Address
Phone/Fax Number	**E-Mail/Web Address**	**May we contact you in the future? (If "Yes," indicate any restrictions)**
(P)	@	☐ Yes: _____ ☐ No
(F)		

2. Please identify which agencies use the radio system.

2.5 Do you have Memoranda of Understanding (MOU) established? If yes, please specify.
.

3. Please provide the following demographic information for public safety system users.

	Number of Radio Users	Number of Stations
Law Enforcement Agencies		
Fire Departments		
EMS Agencies		

II. Current System Infrastructure

4 System Name:_____ Please Check ☐ Share ☐ Own ☐ Both ☐ Lease

If shared, what agencies operate on the system?

_____

If leased, who operates and maintains the system?_____

5. Please provide all general system information (Please check all that apply).

Description	Type
Manufacturer	☐ Motorola ☐ GE ☐ M/A-Com (Ericsson) ☐ EF Johnson ☐ MA-Com (Open Sky) ☐ Other (specify)
Model	☐ EDACS ☐ LTR ☐ MPT 1327 ☐ Project 25 ☐ SmartNet ☐ SmartZone ☐ Open Sky ☐ Other (specify)
What type of trunking protocol is used	☐ Transmission ☐ Message
What type of database management software is used?	
Installer	☐ In-house ☐ Manufacturer ☐ Electronics Shop ☐ Other (specify)
Band (MHz)	☐ 138–144/148–174 ☐ 406–420 ☐ 450–470 ☐ 470–512 ☐ 764–776/794–806 ☐ 806–824/851–869 ☐ Other (specify)
Approximate System Age	
Encryption Capable?	☐ Yes ☐ No

6. Is there any system-related documentation available (e.g., talk group plan, system and/or connectivity diagrams, summary information tables, transmission system information)? ☐ Yes ☐ No If yes, may we have a copy? ☐ Yes ☐ No

7. List all types of mobile radios used on the system.

Manufacturer	Model	Quantity	Approximate Age

8. List all types of portable radios used on the system.

Manufacturer	Model	Quantity	Approximate Age

9. Please describe console equipment.

Manufacturer	Model	No. of Control Channels	No. of Dispatch Positions	Location (address)

10. Describe your communication center(s) console configuration. (e.g., Domain-specific consoles, backup communications center, how are folders set up on Gold Elite consoles?)

11. What system statistics (e.g., busies, delays, calls per hour, quality of service, and peak loading) are collected?

12. How does the system maintain communications during partial and complete failure of the system (e.g., failure of the trunking controller, links to the trunking controller, or individual sites)?

13. Please describe your system maintenance plan (i.e., how often, who performs the maintenance, what is done)

III. Talk Group Information

14. Describe your talk group organization (e.g., common fleets, sub-divided into functional groups).

15. Who was involved in the original fleetmap planning? When fleetmaps need to be changed, who is involved?

16. Since installing the trunked system, have you ever reorganized the talk groups? ☐ Yes ☐ No If yes, please describe the process.

17. On average, how many of the following types of push-to-talks (PTT) occur during a given month?

Types of PTTs	Average Number of PTTs/Month
Mobile-to-mobile	
Private	
Emergency	
Group	
Dispatch	
Telephone interconnect	

18. Describe the priority levels assigned to users and talk groups. (Who receives the highest priority? Forced calls? Emergency calls? Which talk groups have higher priorities than others?)

19. Describe your system capacity:
    Total number of talk groups _____
    Total number of subscriber IDs_____

20. Do users experience congestion on primary operational channels? ☐ Yes ☐ No If yes, describe.

21. Do you have plans for future expansion? ☐ Yes ☐ No If yes, please describe.

22. Please describe recent radio reprogramming efforts.

23. Please describe radio training for users. (How often? What kind of training is offered? Training materials used [May we have a copy?])

24 Please describe radio training for dispatchers. (How often? What kind of training is offered? Training materials used [May we have a copy?])

25. Describe available intrasystem interoperability talk groups. (e.g., “stormplan”)

26. Please describe use of intersystem interoperability talk groups on your system. (Shared talk groups with other trunked systems)

27. Please describe use of regional interoperability talk groups on your system.

28. How is interoperability achieved with agencies that operate on varying proprietary systems, varying technologies, and with varying vendor products?

29. How does the trunked system interoperate with conventional systems (for example, FMARS, PMARS)?

30. How and when are talk groups patched together? (e.g., ad hoc and/or permanent patches)

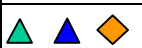
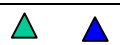
31. Do you use any national or regional mutual-aid channels for achieving interoperability? ☐ Yes ☐ No If yes, please specify.

32. Do you participate in any regional working groups? ☐ Yes ☐ No If yes, please describe. (Which agencies participate? What is the impact to talk group planning?)

APPENDIX C—OPERATING ENVIRONMENT OVERVIEW

Appendix C provides an overview of the operating environment for those agencies consulted for this study. It details the User Domain, which includes the geographical region and number of users served by the agency. The user domain also identifies the missions the trunked radio system supports, the age of the system, the trunking protocol in use, whether or not the system is encryption capable, and the number of talk groups in use. Talk Group Organization identifies who participated in fleet map planning, whether a predefined fleet map exists, and assigned user priority. Database management details the type of system performance monitoring and subscriber ID management used by system administrators. System planning shows whether an agency does or does not use disaster plans and if a future growth plan is in place. System maintenance describes the type of maintenance performed on the system and who performs the maintenance. The interoperability section details how agencies operating on the system achieve interoperability with outside entities.

	Agency	A	B	C	D	E	F	G	H	I	J	K	L
	Geographical Region	Suburban	Suburban	Suburban	Metropolitan	Metropolitan/ Suburban	Suburban	Suburban/ Rural	Metropolitan/ Suburban	Metropolitan/ Suburban	Metropolitan	Suburban	Rural
	User Population	Small	Small	Medium	Medium	Large	Large	Large	Large	Large	Large	Medium	Small
User Domain	Law	√	√	√	√	√	√	√	√	√	√	√	√
	Fire/EMS	√	√	√	√	√	√	√	√	√	√	√	√
	Public Works	√	√	√	√	√	√	√	√	N/A	N/A	√	√
	Age (years)	> 10	> 10	< 5	< 5	< 5	6 to 10	6 to 10	< 5	> 10	< 5	6 to 10	> 10
	Mode of Operation	Mixed	Analog	Digital	Digital	Digital	Mixed	Analog	Mixed	Analog		Analog	Analog
	Trunking Protocol	Transmission	Unknown	Transmission	Message	Transmission	Transmission	Transmission	Unknown				
	Encryption Capable	No	√	√	No	√	√	√	√				
Talk Group Organization	Number of Talk Groups	40	40	238	212	150	350	253	1,000				
	Fleet Map Planning Participants	• Unknown (limited documentation exists)	• Vendor • Limited agency participation	• Agency specific user groups • Vendor representatives • LMR consultants	• Surveyed all participating organizations • Vendor representatives	• Command staff • Radio technical supervisor • Limited documentation exists	• Major study to release RFP • Several senior officials • Agency specific working groups	• Network services project team	• Agency specific working groups • Internal system development team • Vendor representatives • LMR consultants				
	Predefined Fleet Map	√	√	√	None	√	√	√	None				
	Assigned User Priority	No	No	No	No	No	No	No	No				
Database Management	System Performance Monitoring	Ad hoc	No	No	Ad hoc	Monthly	Monthly	Ad hoc	Daily				
	Subscriber ID Management	√	No	√	√	√	√	√	√				
System Planning	Disaster Plan	None	None	√	None	√	√	√	√				
	Future Growth Plan	Limited	√	Limited	None	None	√	√	√				

	Agency	A	B	C	D	E	F	G	H	I	J	K	L
System Maintenance	In-House or Outsourced	Outsource	Outsource	Mixed	In House	In House	Mixed	In House	Mixed				
	Proactive or Responsive	Responsive	Responsive	Proactive	Proactive	Proactive	Proactive	Proactive	Proactive				
	System Failure Tests	None	None	√	√	√	√	None	None				
Interoperability	Internal Solution				Not applicable								
	External Solution				Not applicable								
	Regional Solution				Not applicable								
	Federal Solution				Not applicable								
	P25 Compliant	No	No	√	No	No	No	No	No				
	Participate in Regional Working Groups	√	√	√	√	No	√	√	√				

Key

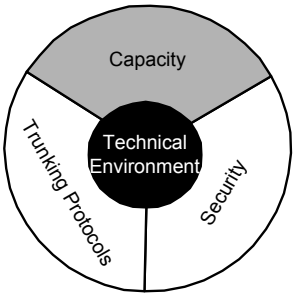
Audio switch	Portable microwave units	First responder vehicle	Shared systems with a limited number of federal users	Trailer (mobile) solution
Radio cache	Mutual aid calling channels	Tactical channels	NPSPAC	Designated emergency talk group
Coordination talk groups	Exchange templates	Share talk groups	Various patching methods	Console-to-console patch

APPENDIX D—KEY TECHNICAL CONSIDERATIONS

APPENDIX D—KEY TECHNICAL CONSIDERATIONS

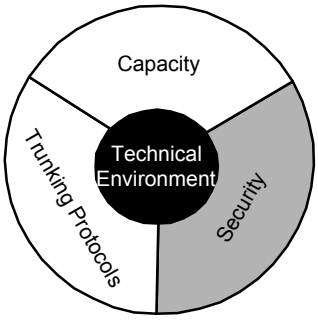
Various technical advantages are associated with installing a trunked radio system. In general terms, trunking is the commonly accepted term for electronically controlled sharing of a relatively small number of communications channels among a relatively large number of users. A detailed explanation of trunking is provided in Appendix A. Based on discussions with radio managers, common system features, including capacity, security, and trunking protocols, emerged as having an operational impact regardless of the system manufacturer. This appendix details each of these common system features.

D.1 Capacity



Capacity, a vendor-specific feature, includes network scalability—the ability to increase system capacity seamlessly, integrate new features, and support new applications. An agency's current and future needs typically determine the type of system selected. For example, a large state system may require a significant number of tower sites (possibly in the hundreds depending on the size of the jurisdiction, topography, and coverage requirements) for adequate coverage. In addition, the system must support a significant number of subscriber identification numbers (i.e., IDs) and talk groups for agencies joining the system after implementation. Conversely, a single jurisdiction or county (again, dependent on size) may need a smaller system. However, it is still necessary that system managers of both system sizes plan for future system growth and monitor system capacity. Additionally, the number of talk groups that can be programmed into subscriber units varies among vendors and radio models.

D.2 Security



As depicted in Figure D-1, various levels of voice privacy are available with trunked land mobile radio (LMR) systems. Voice privacy helps to prevent operational confusion among users by limiting who can hear a message, in three ways—talk group privacy, arbitrary channels, or

encryption. The lowest level of voice privacy available on trunked systems is talk group privacy. Because subscriber units are preprogrammed with talk groups, only users with the talk group programmed into their subscriber units are able to monitor and communicate via that talk group.

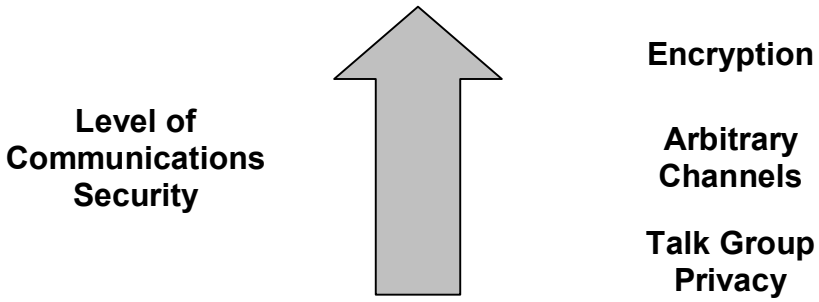


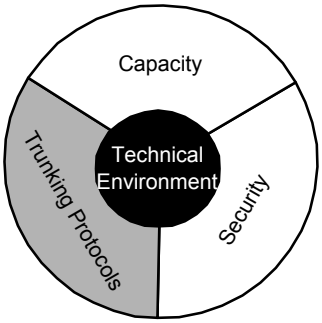
Figure D-1
Voice Privacy Levels

Trunked LMR inherently provides an additional level of voice privacy. Because trunked radio system communications are transmitted on an arbitrary channel selected by the system, it typically becomes difficult for unauthorized users to monitor the voice communication of a particular group of users. However, scanning receivers that are capable of tracking trunked system operations and the arbitrary channel assignments are available to the general public.

Finally, the degree of privacy can be enhanced on a trunked system by adding digital voice encryption, if supported by the system architecture and subscriber units. Specific user requirements, or an agency's mission, typically drive the need for encryption. For example, many law enforcement agencies prefer to encrypt their mission-sensitive voice traffic for specialized units such as a narcotics division or tactical operations teams. Emergency medical services (EMS) may encrypt talk groups specifically used to transmit patient conditions and treatment orders between the hospitals and EMS field units. The subscriber unit encrypts and decrypts communication traffic. Users with encryption-capable radios can also operate in the "clear" mode, permitting communications with users using non-encryption-capable radios. Encryption-capable radios emit a tone to inform the user that they are operating in the clear. If a user of one of these radios receives voice communications in the clear, the encryption-capable radio automatically switches to the clear mode enabling communications. However, a user of an encryption-capable radio must switch his or her subscriber unit to the clear mode before transmitting to a non-encryption-capable radio because the latter radios are not capable of switching modes.

For additional information regarding LMR encryption, readers can reference the Public Safety Wireless Network (PSWN) Program document, *Introduction to Encryption Key Management for Public Safety Radio Systems* on the PSWN Program Web site www.pswn.gov.

D.3 Trunking Protocols



The trunking protocols—transmission and message—detail the "hang time" or length of time a repeater continues to transmit after the user has released the push-to-talk (PTT) button. The PTT button is the switch on a subscriber unit that when pressed causes the subscriber unit to transmit.[5] With transmission trunking, the repeater delay time is set to zero, and every message starts at zero. As a result, the process of assigning channels is repeated every time the PTT button is depressed. From a technical perspective, this method provides more airtime. As depicted in the lower half of Figure D-2, when the first transmission occurs, communications occur on Channel 1, but because of transmission trunking, the second transmission occurs on Channel 3 instead of Channel 1 because the repeater delay time is set to zero. The channel in use is automatically released when a user releases the PTT button.

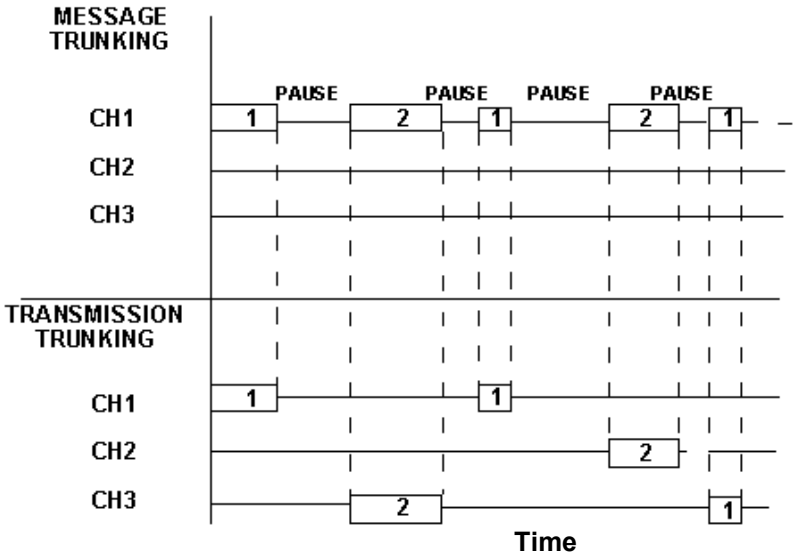


Figure D-2
Message Trunking versus Transmission Trunking[6]

For message trunking, repeaters are typically set to a 3- or 4-second delay meaning that a radio channel is assigned for the duration of the conversation. As depicted in Figure D-2, the

[5] PSWN Program's *Comparisons of Conventional and Trunked Systems*.
[6] http://www.motorola.net.au/what_is.html

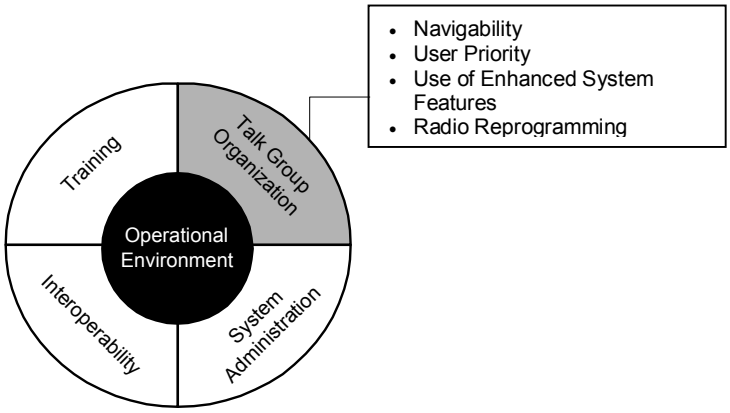
duration of communications that occur on Channel 1 reflects the built-in delay. There is debate in the LMR industry regarding which protocol is better. Some communications officials believe that message trunking is preferred because it eliminates operational confusion by simulating a conventional system. Additionally, message trunking is often considered more suitable for critical situations because a channel is generally required for the duration of the conversation. However, operational and functional requirements may dictate the application of either message or trunking protocols.

APPENDIX E—KEY OPERATIONAL CONSIDERATIONS

APPENDIX E—KEY OPERATIONAL CONSIDERATIONS

Operationally, public safety agencies are presented with an array of challenges relating to system management. These challenges stem from both current and future operational needs that must be addressed to ensure the availability of communications. The Public Safety Wireless Network Program has identified a number of operational considerations as significant to trunked radio systems operations. Specifically, these operational considerations include—talk group organization, system administration, interoperability, and training. This appendix details each of these operational considerations.

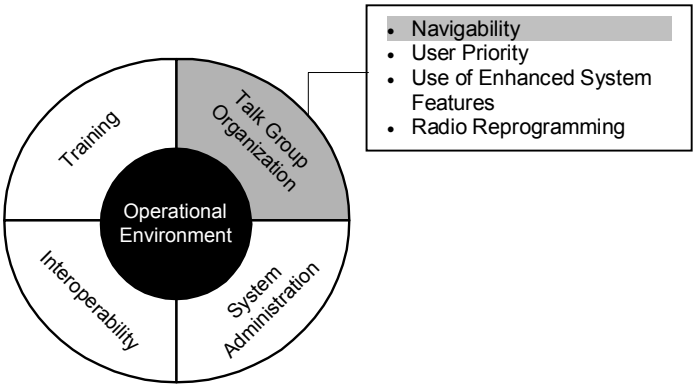
E.1 Talk Group Organization



With efficient fleet map development and talk group planning efforts, trunked land mobile radio (LMR) systems can support a significant number of users and interoperability opportunities. Fleet map development is the process of producing an operationally useful talk group structure and is further detailed in Section E.2. The organization of talk groups impacts basic user communications as well as interoperability. However, extensive preparation is required to develop an effective talk group plan. If designed and executed properly, an effective talk group plan will enhance existing system capabilities and provide flexibility over the long term. Important elements to consider when developing talk group plans include—

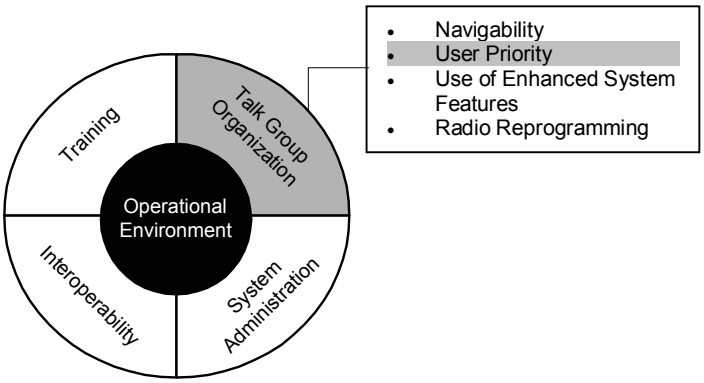
- Navigability
- User Priority
- Use of Enhanced System Features
- Radio Reprogramming.

- ***Navigability***



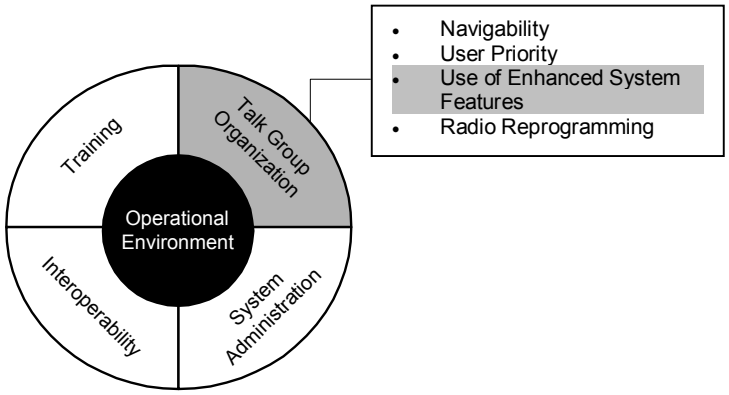
For optimal support of public safety missions, it is important to balance the number of talk groups with an acceptable number of users. To do this, a system manager must consider both the size and the number of talk groups. Talk group size refers to the number of users that can communicate effectively using one talk group, a number that varies depending on the frequency and duration of communications. The number of established talk groups is also important because if too many talk groups are established, users may experience long delays before their talk group is assigned a channel. Additionally, establishing an abundance of talk groups may negatively affect navigability of the talk group plan by users because of the difficulty associated with locating the correct talk group needed for communications.

- ***User Priority***



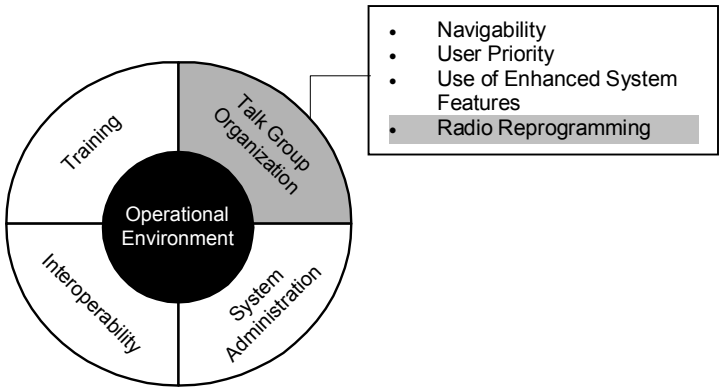
Priority levels allow users or groups to access the system ahead of others when the system is busy. Priority levels are typically used on systems supporting both public safety and public service communications to ensure priority access to public safety agencies during an incident requiring a significant number of first responders. Generally, the highest priority, 1, is reserved for emergencies. The emergency action button is typically given priority 1 on most systems. During activation, the dispatch center is notified immediately with an audible tone and visual display when the user depresses the emergency button. Priorities 2 through 10 are assignable by the system manager on a system, talk group, or per radio basis.

➢ ***Use of Enhanced System Features***



The use of enhanced trunking features, such as private call, call alert, priority scan, multiple scan lists, telephone interconnect, and dynamic regrouping, should also be considered when establishing talk groups because of the potential impact on system performance. "Private call" allows two radio users to create a temporary two-person talk group. "Call alert" allows a user to "page" another subscriber device. "Priority scan" allows the definition of a primary talk group that the subscriber unit will return to when there is activity. Some vendors provide equipment that will allow the definition of multiple different lists of talk groups to be scanned. "Telephone interconnect" provides the ability to connect a subscriber unit directly to the public switched telephone network. "Dynamic regrouping" allows the subscriber unit to be placed into a private group through manipulation of the system control console. However, several of these features may degrade system performance substantially if multiple users employ the feature at the same time. Therefore, it is essential that the system manager closely monitor the use and allocation of these enhanced system features.

➢ ***Radio Reprogramming***

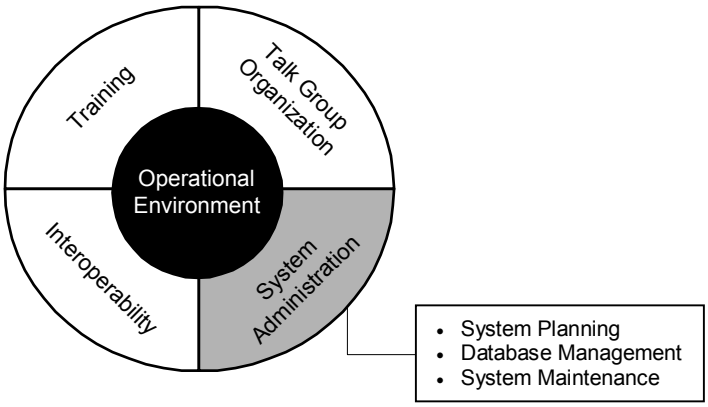


Radio reprogramming is essential to accommodate the technical and operational changes agencies institute. As a trunked radio system is modified, reconfigured or updated, each portable and mobile radio affected by the change must be reprogrammed to reflect the most current system configuration information. Standard changes include reorganizing the system's fleet map and exchanging or reallocating subscriber IDs. In addition, targeted reprogramming may be required to facilitate the tactical communications needs of the organization during a preplanned event or emergency incident or with inclusion of new field personnel. To reprogram radios, an

agency must possess the necessary equipment, which includes a computer, reprogramming software, and the cabling required to connect the computer and radios. As new radios are introduced into the agency's equipment complement, there also may be requirements to update or acquire additional cabling and new programming software. Radio reprogramming can be a time-consuming process consisting of labor hours for one to several programmers, depending on the size of the agency. Some of this time can be mitigated using over-the-air-programming features, if the vendor and the system support this capability.

However, if an agency does not possess the equipment, human resources, or intellectual capital to reprogram radios, it may be necessary to solicit vendor assistance. Agencies must ensure that system modification or talk group reorganization is planned properly and vigorously tested to reduce the need for rework or additional changes once reprogramming is complete. In addition, agencies must consider the regional implications of talk group modifications because an entire region's radios may require reprogramming as a result of even a minor change. Therefore, reprogramming efforts should be coordinated regionally to sustain interoperability and maximize efficiency.

E.2 System Administration

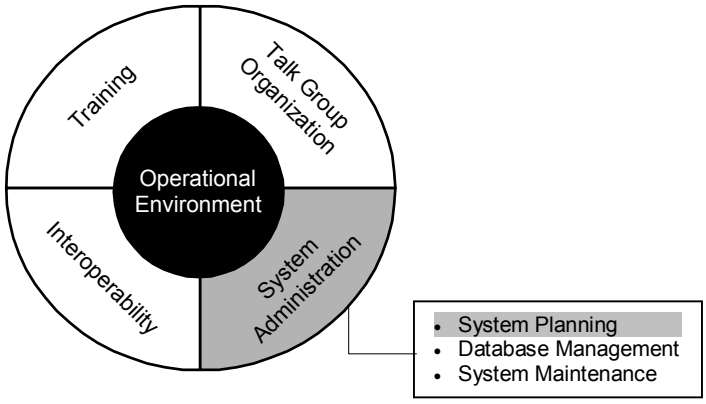


System administration has become increasingly important to the effective management of a trunked LMR system. As such, the primary administrative responsibility of a system manager is to ensure efficient and reliable delivery of critical communications. Specifically, this responsibility includes—

- System Planning
- Database Management
- System Maintenance.

To perform these tasks efficiently, system managers must have a comprehensive understanding of the day-to-day operational and technical aspects of trunked radio systems. In addition, when considering or implementing interoperability with other public safety agencies from multiple levels of government, a new layer of complexity is added to system administration. Today's system managers must focus not only on the operation and administration of their own radio system, but also on that of other agencies with which interoperability is required or desired.

➢ ***System Planning***



To realize the benefits of system planning in the LMR environment, planning must occur in the context of the organization as a whole. While end user requirements are a major consideration throughout the system planning process, the focal point of this process should be the mission of the organization. Because the mission of public safety agencies entails protecting lives and property, interoperability may likely be at the forefront of the planning process and involve those agencies inside and outside of the organization with which interoperability is currently needed or may be needed in the future. By involving agencies regionally, a unified long-term plan can be established that considers the interests of each agency involved. The plan should consist of an approach that prepares the organization for possible change and focuses on several key aspects of system planning for trunked radio systems—fleet mapping, disaster planning, interoperability planning, and forecasting future growth.

- **Fleet Mapping—**Fleet mapping consists of gathering and evaluating the operational, functional, and technical requirements of the agencies involved and those of the user community to produce a logical talk group structure that considers the internal and external communications needs of each agency. The fleet map may need to be redesigned to accommodate organizational changes as they occur. Disaster and interoperability planning and forecasting future growth are all integral parts of fleet map development.

- **Disaster Planning**—Disaster planning entails preparing a communications plan, commonly referred to as a "stormplan," for natural disasters, large emergencies, or special events before they occur. In preparation for a disaster or event, agencies typically perform field exercises to logistically organize and practice for disasters and install backup and supplementary equipment at alternate sites to sustain communications during system failure.

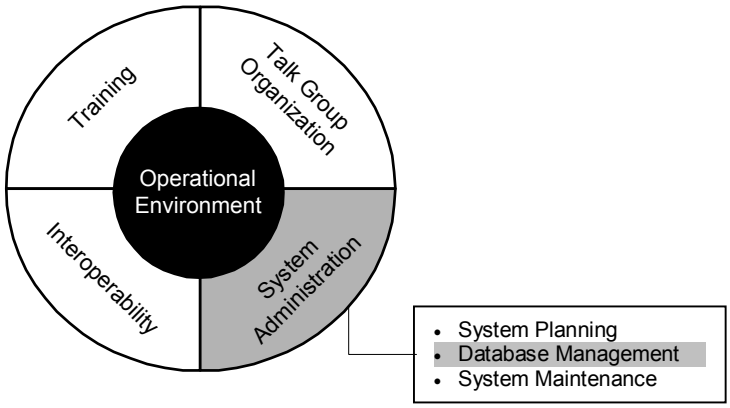
- **Interoperability Planning—**Interoperability Planning should be performed throughout the system lifecycle,[7] initially during the system design process and later

[7] The system lifecycle describes a step-by-step process that system planners use to plan, design, and procure LMR communications systems.

as necessary. Specifically, interoperability planning includes coordinating with internal and external agencies with which interoperable communications are required, determining the appropriate technical solution, and training users.

- **Forecasting Growth—**In addition, public safety agencies should plan for future growth so as not to expand beyond system capacity, which could result in interference among users, system busy tones, or a lack of physical space available to accommodate the additional equipment that may be required. The size and location of the jurisdiction or region is a major factor in determining the future growth of the system. By continuously planning, system managers can mitigate potential barriers to seamless communications and successfully position the organization for future change.

➢ ***Database Management***

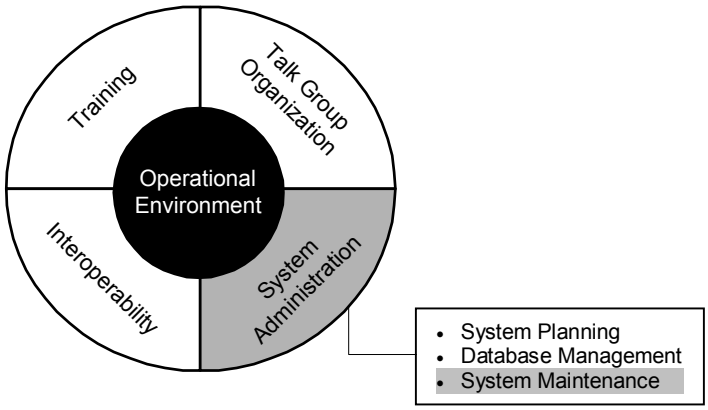


System managers monitor and manage the system database to track system statistics and resources. The system database serves as a central repository of system-related information such as the number of push-to-talks (PTT) activations, channel and talk group usage, and some enhanced feature monitoring—all of which are received from the system controller. Using network management tools, system managers can analyze system data and generate statistics to determine peak loading times and monitor system data such as interference among users, system busy tones, and traffic patterns. These tools, which can be acquired from vendors, or for simple applications, downloaded from the Internet, enable the manager to better understand the system, and in turn, reallocate resources to improve overall system performance.

The system database may include IDs, which correspond to each subscriber unit on the system. Subscriber IDs are a series of alphanumeric characters. Because of the relational characteristics of a database, an alias (i.e., name of division, person) can be assigned to each subscriber ID to identify the individual using a particular unit. Therefore, each time an individual pushes the PTT button, his or her alias will be logged into the system database along with a time/date stamp; thereby, providing the system manager with a detailed look at individual usage patterns. Without an alias assignment, PTTs will be logged with the multidigit alphanumeric ID number. In some regions, the existing need for and prevalence of interoperability requires agencies to share subscriber IDs with a number of other agencies. This reality necessitates a well-organized approach to subscriber ID management and is especially

critical for large agencies because of the quantity of subscriber IDs that must be managed. To facilitate this effort, system managers can develop their own means of tracking subscriber IDs using simple applications, such as database tools or spreadsheets. These applications permit system managers to avoid assigning duplicate subscriber IDs and to facilitate the assignment of IDs internal and external to their own organization.

- ***System Maintenance***



To guarantee a high quality of service, system managers must conduct system maintenance on a regular basis. There are two main aspects of system maintenance: routine maintenance and fault management.

- **Routine Maintenance—**Routine maintenance, or preventative maintenance, consists of inspecting the condition of equipment and software, troubleshooting problem areas, and addressing any other aspect related to the normal "wear-and-tear" on the system. Routine tasks may include inspecting antennas, antenna connections, coaxial lines, grounding systems, tower structures and lighting, equipment shelter integrity, and emergency and backup power systems. In addition, impending failures can be detected by monitoring sites and using built-in reporting and control systems. Routine maintenance enables the system manager to anticipate potential obstacles to service availability and optimize the technical performance of the system.

- **Fault Management—**Fault management includes managing any task related to the potential failure of the system. System failure could occur for several reasons, including equipment failure, software failure, natural disasters, sabotage, or any other unforeseen circumstance. Upon failure, the trunked LMR system generally either converts to site trunking[8] or operates in "fault tolerant"[9] mode, depending on the particular malfunction. Site trunking indicates that a repeater has lost its connection to the system controller and enables the system to operate in a reduced capacity while still trunking calls. Depending on how subscriber units are programmed, the user can often scan for and operate on an alternate site that is working properly until the

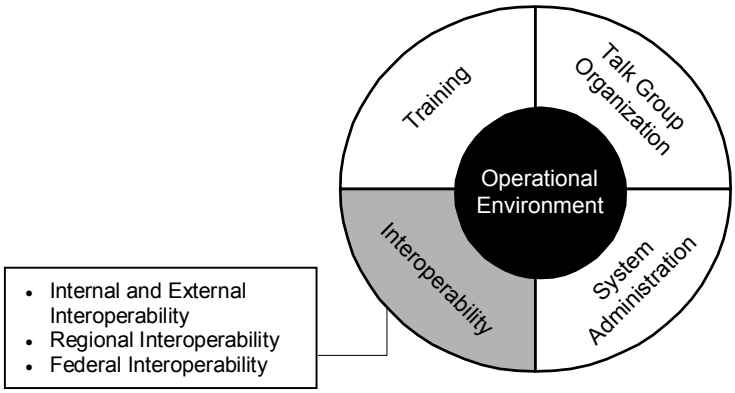
[8] Site trunking occurs when a transmitter loses the ability to communicate with the zone controller. Radios can only communicate with other radios affiliated with that site.
[9] Fault tolerant mode occurs when the transmitter site with which a radio is affiliated fails and cannot perform trunking, causing the radio to switch automatically to a predetermined frequency.

problem is corrected. Fault tolerant mode occurs when a site's controller goes out of operation. In contrast to site trunking, during fault tolerant mode, each radio using that site converts to conventional mode and operates using a conventional frequency. Whether the system goes into site trunking or fault tolerant mode, public safety agencies require 24-hour-a-day, 7-day-a-week rapid response to repair the system and restore normal operation.

System maintenance can be outsourced, performed in house, or achieved through a combination of the two, depending on the level of service required by an agency and the level of staff expertise. By outsourcing system maintenance responsibilities, technical experts with vendor-specific experience perform system maintenance. Outsourcing may allow an agency to take advantage of economies of scale and to stabilize costs due to the predictability of system maintenance functions, which in turn could alleviate large capital outlays required for systemwide replacements. In addition, outsourcing may reduce the risk of "do-it-yourself" fixes that can cause delays and additional problems.

Conversely, in the event of system failure, because rapid response is essential and can be time consuming due to the level of coordination required between an agency and a service provider, in-house maintenance may be better suited for some agencies. In-house maintenance can be less expensive than outsourcing and is preferred by most agencies that operate a repair shop and have technical experts on staff. However, the costs to acquire technical experts and set up and maintain a repair shop including cost of space, tools, test equipment, spare parts, and service vehicles must be considered. Because certain agencies may possess some but not all resources necessary to perform system maintenance, agencies can outsource some tasks and perform others in house. Many potential partnerships and agreements can be established with a service provider for system maintenance; each should be evaluated in the context of the specific agency's resources and requirements.

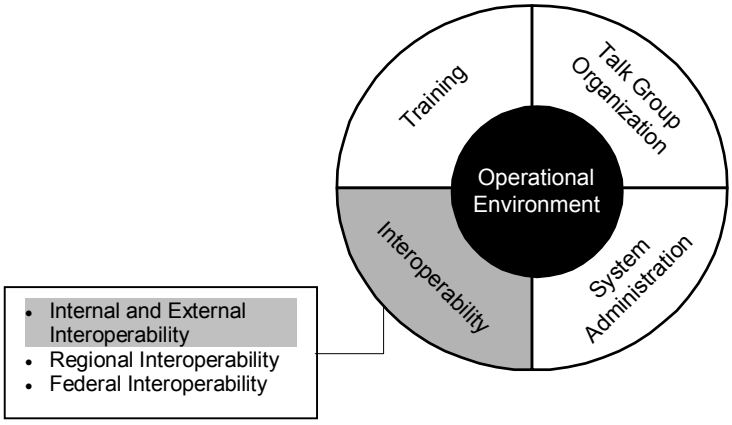
E.3 Interoperability



Virtually all local, state, federal, and tribal public safety agencies require wireless communications interoperability for both emergency and day-to-day operations. Interoperability is defined as the ability of public safety personnel to communicate by radio with staff from other agencies, on demand and in real time. This sections highlights the following—

- Internal and External Interoperability
- Regional Interoperability
- Federal Interoperability.

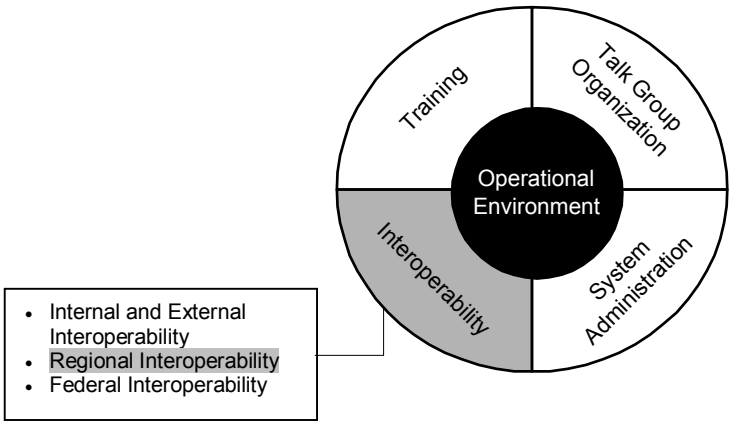
➢ ***Internal and External Interoperability***



Regardless of the type of interoperability, public safety agencies are all working to achieve the same mission—safe, efficient protection of life and property. To that end, agencies must coordinate internally and externally to identify and alleviate interoperability shortfalls. They must begin by addressing interoperability internally to ensure those organizations inside their city or county using the same system can communicate with one another during both day-to-day and emergency operations. This form of internal interoperability extends to regional systems used by multiple organizations crossing jurisdictional boundaries. These organizations can include local fire departments, emergency medical services, law enforcement agencies, and public works organizations.

There are a number of methods for achieving internal interoperability between organizations operating on the same trunked system. For example, an agency could program a coordination talk group into each subscriber unit on the system. During an emergency incident, this talk group could serve as a central point of communications for responders to organize and manage the incident. Coordination talk groups are one method of achieving interoperability between agencies with disparate missions from multiple jurisdictions. However, it is important to note that agencies from multiple jurisdictions within the same county may have different operating procedures. Thus, agencies should coordinate internally to develop an effective interoperability solution.

➢ ***Regional Interoperability***



Public safety agencies can seek to partner with one another regionally in order to break down barriers to interoperability. Regional interoperability is the ability for agencies from a wide area or region to communicate with one another. By partnering to solve problems regionally, agencies can realize the benefits of strategic and tactical alliances that facilitate interoperability. Together, agencies can build relationships with one another to identify common interoperability issues. As a result, they can pool their resources to address these regional interoperability issues, thereby maximizing the use of available resources.

A number of common regional interoperability solutions are used by agencies operating trunked radio systems, including sharing talk groups and using national calling and tactical channels. Sharing talk groups refers to agencies allowing a talk group from their own system to be programmed into the radios of other agencies in the region. When an emergency incident that requires mutual aid assistance occurs in one jurisdiction, agencies from surrounding jurisdictions can switch their radios to that agency's talk group and communicate on that agency's system for the duration of the response. However, this interoperability solution requires that subscriber units from each agency have available capacity to store the mutual aid talk groups, that the trunking protocols are compatible, and that their home system extends coverage to the incident area. Although interoperability solutions such as talk group sharing between local agencies are suitable for localized mutual aid operations, they are short-term fixes and may be inadequate when outlying agencies are called in to assist.

National calling channel, another common regional interoperability solution, permit all agencies that have the channels programmed into their system to communicate with one another regardless of geographic location. As illustrated in Figure E-1, when using national calling and tactical channels, Agency B can communicate on Agency A's system independent of its home system coverage area. Depending on the frequency band used, some agencies may be required to purchase new equipment to communicate on the national calling channels. System managers must coordinate the use of repeaters on these frequencies between regional agencies to minimize the potential of interference generated by multiple active repeaters in close proximity.

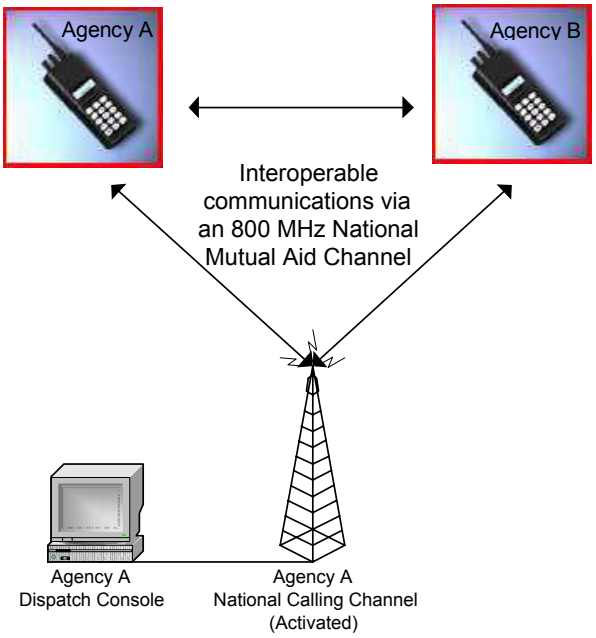
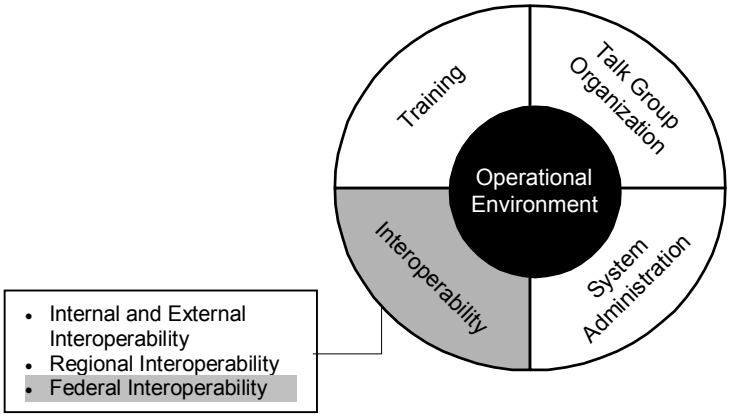


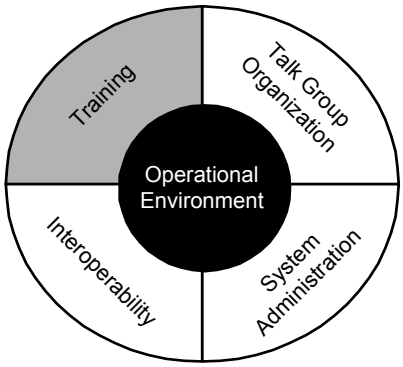
Figure E-1
Operating 800 Megahertz National Mutual Aid Channels

- ***Federal Interoperability***



Geographical location and mission requirements often necessitate interoperability with federal agencies. For example, federal agencies have a greater presence in border and maritime response scenarios. This prominence, coupled with the mission of federal law enforcement in these areas, highlights the need for interoperability with federal agencies in certain regions. It is important that agreements and procedures are developed among local, state, and federal agencies to ensure a viable interoperability solution exists should a major emergency incident occur.

E.4 Training



Communications training is an important operational element of trunked LMR systems. LMR engineers, radio technicians, dispatch personnel, and field users each require training tailored to suit their respective operational mission. However, communications training comprises both technical and operational components. By design, the basic operation of some components of LMR radio systems, such as consoles, and portable and mobile radios are intuitive; however, many valuable features are not obvious and require some training. For example, many users require training for enhanced features such as scan, call alert, and private call. Beyond the technical considerations, users require additional procedural training. Field users will likely need to be trained regarding radio transmission guidelines for day-to-day operations, mutual aid responses, and emergency incidents. The radio technician should be trained to abide by operating procedures governing portable radio deployment and maintenance tasks.

Depending on communications training requirements, agencies may develop content and select delivery methods that encompass a variety of training scenarios. Vendor representatives, a train-the-trainer[10] arrangement, or in-house expertise can provide suitable training for most users in one-on-one, and/or group settings.

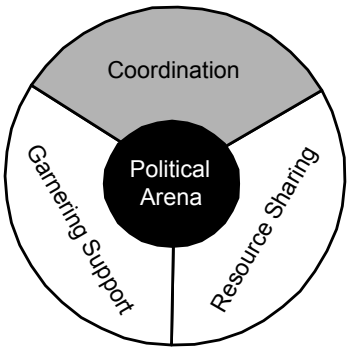
[10] Placing employees with training responsibilities in an instructional setting with a vendor or other informed source forms the "train-the-trainer" arrangement. These employees should acquire the skills and knowledge necessary to develop and deliver a training module tailored for the organization's users.

APPENDIX F—KEY POLITICAL ARENA CONSIDERATIONS

APPENDIX F—KEY POLITICAL ARENA CONSIDERATIONS

The public safety political arena is filled with implications for the radio user, technician, and stakeholder. Regardless of technology, the political environment influences the planning, funding, implementation, maintenance, and future of a land mobile radio (LMR) system. More importantly, the political environment impacts the approach public safety organizations may take in establishing or improving wireless interoperability. Specifically, this approach involves coordinating with other organizations, sharing resources where appropriate, and garnering stakeholder support and user acceptance.

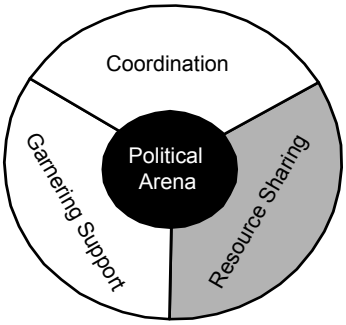
F.1 Coordination



LMR system operations can become a source of conflict due to the potential for large user populations with dissimilar missions and levels of authority. Coordination and cooperation among system participants is critical to ensuring effective, overall LMR system operations. In addition to operations, coordination is critical to ensuring interoperability among public safety agencies from all levels of government. Proper coordination should result in a unified approach to solving interoperability issues allowing agencies to work jointly to develop joint solutions for each agency involved. As a result of this effort, agencies can develop agreements to define and establish interoperability partnerships. Memoranda of understanding and mutual aid agreements are two ways agencies can establish responsibilities and contractual obligations to support operations and interoperability.

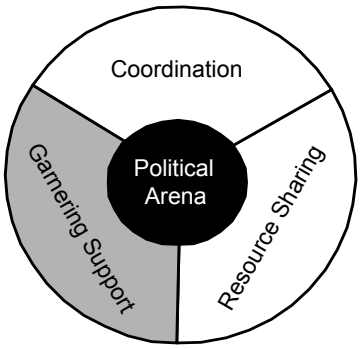
Public safety agencies can also coordinate to develop short-and long-term strategies for addressing operational and interoperability issues. By examining the various operational objectives and interoperability requirements of each agency, planners can identify common problems that must be addressed. To focus on the operational and interoperability requirements of the various organizations, agencies should design short- and long-term strategies for addressing these issues. As part of a short-term strategy, agencies can develop procedures for on-scene communications based on their current system capabilities. In addition, agencies could explore short-term interoperability solutions to fulfill their requirements until such time as they can establish a long-term solution . Long-term strategies should focus on the future goals and requirements of all agencies involved. Because of the numerous operational and interoperability benefits that can be realized, agencies often consider the development of a regional or statewide system to satisfy their long-term needs.

F.2 Resource Sharing



One of the key outcomes of effective coordination is resource sharing, which often results in increased efficiencies and reduced costs. By sharing resources, agencies can realize economies of scale resulting in advantages such as reduced operations and maintenance costs and lower costs to obtain advanced technologies. Two resources agencies commonly share are spectrum and infrastructure. Sharing spectrum allows agencies to more efficiently use the limited radio frequency spectrum available to public safety agencies. In addition, sharing infrastructure reduces cost, but most importantly, positions agencies for interoperability through the inherent advantages of operating on the same infrastructure.

F.3 Stakeholder Support



Before making decisions regarding system procurements and enhancements, agencies should gain stakeholder support as well as user acceptance. Depending on the specific change required, a number of personnel could be impacted, from field users to legislative officials responsible for allocating funding for the proposed change. Therefore, it is important to build consensus among all individuals affected by the change. For example, if two agencies join together to develop a shared, regional system, the idea should first be presented to and discussed with the user community to gain their acceptance of the proposed change. Next, the two agencies should coalesce to present their proposal to senior decision makers responsible for funding the initiative. Typically, when stakeholders and users are involved in the system planning and enhancement process, they are more likely to accept the system and the resultant operational changes. Therefore, it is important for the system manager to balance political considerations and garner user and stakeholder acceptance.

APPENDIX G—PROJECT 25

APPENDIX G—PROJECT 25

To address the problem of a lack of interoperability between various public safety agencies and enhance the usage of scarce spectrum resources, the Association of Public Safety Communications Officials, Inc. (APCO) established Project 25 (P25) in 1989. This effort brought together representatives from local, state, and federal governments and three associations—APCO, the Association of Telecommunications and Technology Professionals in State Government (NASTD), and the Telecommunication Industry Association (TIA)—to define a set of common technical standards for land mobile radio (LMR) systems, critical for public safety communications. The end goal is to define a set of common standards that would allow any manufacturer to produce standards-compliant equipment compatible with system infrastructures and other disparate subscriber units.

Additionally, the P25 suite of standards would likely increase competition and subsequently lower overall prices of infrastructure and subscriber equipment. P25 efforts are also intended to provide buyers with a choice so that they are not "locked in to" a proprietary system from a single manufacturer. This latter situation occurred after the development of the Project 16 standards, which were the predecessor standards to P25. The following are five objectives of the original P25 standard—

- Spectral efficiency using narrowband channels
- Interoperability between agencies and different levels of government
- Backward compatibility
- Graceful system migration (forward and backward)
- Scalable trunked and conventional capabilities.

Presently, P25 is the only officially recognized public safety digital radio standard applicable to the North American marketplace offering criteria to both conventional and trunked LMR environments.

Standards development can be a tedious and lengthy process and in many cases is primarily controlled by the product manufacturers. The P25 steering committee is responsible for engaging and defining the user needs and criteria and developing a statement of requirements. In support of these efforts, the steering committee and other proponents of P25 standards place great importance on the needs of the public safety user community when developing the technical specifications. The development efforts center on determining the most effective and efficient solutions applicable to the public safety community. The standards are then written to ensure that manufactured equipment used by public safety personnel will operate effectively in both normal, day-to-day operation and critical situations.

The P25 standards are developed with guidance from TIA, whose standards development committees include manufacturer representatives. TIA standards are developed using open procedures that are required by the American National Standards Institute (ANSI). The resulting standards are commonly known as ANSI/TIA/Electronics Industry Alliance (EIA) Series 102, 902, and 905 standards.

P25 is not a single standard for LMR, but rather is a suite of standards documents defining a number of individual criteria and technical specifications for conventional, or trunked, digital communications systems. The standards also speak to the use of encryption, as well as the ability to carry data transmission with voice traffic. Presently, more than 33 standards, systems bulletins, and white papers have been created discussing digital LMR technology for public safety and other commercial markets.

The P25 standards suite now includes a comprehensive 12.5 kilohertz (kHz) and 6.25 kHz Frequency Division Multiple Access standard to achieve greater spectrum efficiency by "narrowing" the bandwidth necessary to transmit a message. The P25 suite will soon include 12.5 kHz two-slot Time Division Multiple Access standards and data communications standards for the newly allocated 700 megahertz (MHz) band.

One of the most recognized P25 standards is the Common Air Interface (CAI). This standard specifies the type and content of the transmission signals of compliant radio equipment. The intent of this standard is to allow any compliant radio, regardless of manufacturer, to communicate with any other compliant radio. The use of P25 CAI compliant radios provides increased opportunities for interoperability between disparate equipment and is the only existing standard offering a direct mode of communication as a part of the CAI.

Another recognized P25 standard is the use of digital voice technology instead of older, analog technology. P25 uses a specific method of digitized voice technology called Improved Multiband Excitation (IMBE). The IMBE voice encoder-decoder, or vocoder, samples the audio input and only transmits certain characteristics that represent sound. The receiver uses these characteristics to produce a synthetic representation of the originally inputted sounds. The applicable standards specify exactly how the IMBE vocoder samples the information, as well as the structure and transmission of the synthesized sound.

The P25 standards define a technology platform that provides the end user mobile and portable radio equipment that incorporates advanced features and functionality such as priority calling, call alert, and group calling between subscriber equipment. The standards also define opportunities to support multiple levels of encryption and security services. These include end-to-end or subscriber-to-subscriber encryption methods employing the Digital Encryption Standard protocols, and in the future, Advanced Encryption Standard protocols. Additionally, P25 standards also discuss the federal government's digital-based cryptographic categories—Type 1, Type 2, Type 3, and Type 4. Type 1 is for U.S. classified material (national security), Type 2 is for general federal interagency security, Type 3 is for interoperable interagency security between local, state and federal agencies, and Type 4 is for proprietary solutions. Over-the-air-rekeying, the method used to refresh the security parameters within subscriber equipment is also supported and defined with the P25 standards.

The past few years have witnessed an increase in acquisition and deployment of P25 compatible and compliant systems. A *compliant* system is defined as a system that supports all the required P25 standards. In contrast, a *compatible* system may only support some of the standards defined within the suite. Manufacturers have developed systems and products that can be compatible *and* compliant. In some cases, fully compliant systems can be deployed but are

initially operated as compatible to allow a graceful migration to the new infrastructure. Also, the P25 standards specify criteria regarding which characteristics are required and which are optional. Manufacturers develop products that incorporate the required standard, optional standards, as well as proprietary value-added features or functions. When contemplating the acquisition of P25 standards based products, buyers should examine fully the standards compliance and compatibility claims offered by the manufacturers.

As more of these systems are placed into service by both public safety and commercial users, manufacturers are recognizing the increased demand, and are responding by providing equipment supporting the defined standards. The increase in equipment offerings by various manufacturers should provide additional opportunities for competition that will benefit acquiring agencies. In addition, the P25 standards can assist in graceful migrations from existing legacy (i.e., analog) systems to the new digital trunked and conventional systems offerings; thereby, extending the valuable lifecycle of existing systems and extending the timeline of new equipment purchases.

Although the P25 standards and the resulting technology developed to comply with those standards provide an opportunity to enhance interoperability between disparate systems and technologies, they should not be viewed as the ultimate solution for public safety's interoperability challenges. While it has been proven that various manufacturers' subscriber equipment can operate effectively on P25 standards-based infrastructure, presently this operation must take place within the same frequency band. A P25 compliant very high frequency portable radio cannot operate on a P25 compliant 800 MHz system without the aid of other interoperability solutions such as console patches, audio switches, or other technical interoperability aids. The P25 standards do take into account the future opportunities for the use of crossband transmitter and receiver equipment to further enhance interoperability between disparate frequency bands. However, there is still no one, simple solution to interoperability across multiple frequencies or band allocations.

APPENDIX H—LIST OF ACRONYMS

APPENDIX H—LIST OF ACRONYMS

ANSI	American National Standards Institute
APCO	Association of Public-Safety Communications Officials, Inc.
CAI	Common-Air-Interface
EIA	Electronic Industries Alliance
EMS	Emergency Medical Services
FCC	Federal Communications Commission
IDs	Identification Numbers
kHz	kilohertz
IMBE	Improved Multiband Excitation
LMR	Land Mobile Radio
MHz	Megahertz
NASTD	National Association of Telecommunications and Technology Professionals in State Government
OTAP	Over-the-Air-Programming
OTAR	Over-the-Air-Rekeying
P25	Project 25
PSWN	Public Safety Wireless Network
PSTN	Public Switched Telephone Network
PTT	Push-to-Talk
SOP	Standard Operating Procedure
TIA	Telecommunications Industry Association