STATEMENT OF WORK

RADIO NETWORK TECHNICAL SUPPORT SERVICES

March 2012
# Table of Contents

## Section I - Introduction

## Section II - Background

## Section III - Scope of Work

### 01 Overview of Services

### 02 Transition Services

<table>
<thead>
<tr>
<th>Service Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide Non-Disclosure Agreements</td>
<td>8</td>
</tr>
<tr>
<td>Update, Deliver, and Implement a Transition Plan</td>
<td>8</td>
</tr>
<tr>
<td>Present Qualified Candidates</td>
<td>8</td>
</tr>
<tr>
<td>Collect and Document the Current Radio Network Environment</td>
<td>9</td>
</tr>
<tr>
<td>Review Operating Processes and Procedures</td>
<td>9</td>
</tr>
<tr>
<td>Develop and Implement Contract Performance Metrics</td>
<td>9</td>
</tr>
<tr>
<td>Radio Safety Training</td>
<td>10</td>
</tr>
<tr>
<td>Prepare Required Reports</td>
<td>10</td>
</tr>
</tbody>
</table>

### 03 Base Services

<table>
<thead>
<tr>
<th>Service Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positions Required</td>
<td>10</td>
</tr>
<tr>
<td>Radio Technology Training Required</td>
<td>12</td>
</tr>
</tbody>
</table>

### 04 Supplemental Services

<table>
<thead>
<tr>
<th>Service Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplemental Repair Services</td>
<td>13</td>
</tr>
<tr>
<td>Supplemental Construction Services</td>
<td>13</td>
</tr>
<tr>
<td>Supplemental Consulting Services</td>
<td>13</td>
</tr>
<tr>
<td>Contract Services Call Order</td>
<td>14</td>
</tr>
</tbody>
</table>

### 05 Contract Administration

<table>
<thead>
<tr>
<th>Service Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of Performance</td>
<td>14</td>
</tr>
<tr>
<td>Required Hours of Operation</td>
<td>14</td>
</tr>
<tr>
<td>Other Support Contracts</td>
<td>15</td>
</tr>
<tr>
<td>Contractor Provided Resources – Base Services</td>
<td>15</td>
</tr>
<tr>
<td>Authority Provided Resources</td>
<td>16</td>
</tr>
<tr>
<td>Reporting Requirements</td>
<td>16</td>
</tr>
<tr>
<td>Key Personnel</td>
<td>17</td>
</tr>
<tr>
<td>Removal of Staff</td>
<td>18</td>
</tr>
</tbody>
</table>

## Section IV - Deliverables

### 01 Plans and Other Documents

### 02 Personnel

### 03 Periodic Reports

## Section V - Appendices

- Appendix A - Organization Chart MA-630
- Appendix B - Chart of Current Staff Functions
- Appendix C - Equipment & Systems List
- Appendix D - Labor Categories and Description
APPENDIX E - CONTRACT POSITION DESCRIPTIONS
APPENDIX F - CONTRACT SUPPLIED ITEMS – PARTIAL LIST
APPENDIX G - INFORMATION SECURITY STANDARD
APPENDIX H - PSWN BEST PRACTICES
APPENDIX I - PSWN RECOMMENDED SECURITY POLICY
APPENDIX J - RESPONSIBILITY FOR ASSIGNED PROPERTY
APPENDIX K - SMARTPHONE WAIVER FORM
APPENDIX L - INTEROPERABILITY WEB EXHIBIT
APPENDIX M – CALL ORDER FORM
SECTION I - INTRODUCTION

The Metropolitan Washington Airports Authority (the Authority) operates and maintains multiple radio communications systems that support Public Safety, Operations, Engineering, Maintenance and other authorized users at Ronald Reagan Washington National Airport (DCA), Washington Dulles International Airport (IAD) and along the Dulles Toll Road/Access Highway (DTR).

The purpose of this solicitation is to acquire an experienced contractor to provide effective radio network technical support services to the Authority’s multiple mission critical radio systems. Working with members of the Authority Wireless and Radio Systems Department in a collaborative manner the Authority seeks a contractor to:

- Provide quality technical support services to the Authority trunked and conventional radio networks and supporting systems
- Provide project management services for Departmental Projects
- Ensure organization-wide standards are developed, maintained, and enforced

The Authority and its radio networks operate in a very dynamic environment where changes are constantly being made. The contractor must be prepared for such changes and both embrace them and react accordingly. For example, currently, the Authority is receiving equipment to implement a 700 MHz radio network for Authority use (section II.D below). This new system will be operational in 2012. This example is provided to give Offerors a sense of the dynamic nature of the Authority Radio Networks.
SECTION II - BACKGROUND

The Authority is a public body politic and corporate, created with the consent of the Congress of the United States by the District of Columbia Regional Airports Authority Act of 1985, as amended, and Ch. 598, Virginia Acts of Assembly of 1985, as amended. The purpose of this entity is to plan, provide, and actively manage world-class access to the global aviation system in a way that anticipates and serves the needs of the National Capital area. The Authority employs approximately 1400 personnel that include a central organization administration, airport management and operations, and Public Safety. The Authority operates from two locations: Washington Dulles International Airport (IAD) and Ronald Reagan Washington National Airport (DCA). For additional information, Offerors are encouraged to visit the Authority’s website at http://www.mwaa.com.

The Authority’s Wireless and Radio Systems Department (MA-630) manages and maintains the Authority’s mission-critical 700/800 MHz Trunked Radio Communication Systems, an extensive 800 MHz in-building and tunnel “Supplemental Radiating System” (SRS), and conventional Authority radio systems that provides radio communications to Authority users, transportation services and Mutual Aid constituencies surrounding the facilities. The principal location for the Radio and Wireless Department offices is Hanger 5, Reagan National Airport. A satellite office is maintained at Dulles Airport.

The mission of the Department is to manage, maintain, and evolve mission critical, radio communication systems to support all user groups operating on the Authority shared, limited resources and adjacent systems. This includes the primary 800 MHz Authority radio system that serves the outside properties, as well as the extensive in-building radio systems that provide reliable communications systems within the structures. A Departmental organization chart for MA-630 can be found in Appendix A and a functional organization chart is provided in Appendix B.

A. Department Goals include:

1. Maintaining 100% core uptime of the primary Authority radio systems
2. Maintaining compliance with FCC Rules and Regulations
3. Providing responsive 24x7 technical support to critical users
4. Providing radio frequency spectrum management services for licensed Authority systems
5. Providing communication system plan review
6. Developing, Implementing and Maintaining backup radio systems and operating plans
7. Determining/resolving radio interference
8. Planning, budgeting and implementing radio system improvements
9. Providing user training

B. The primary Airports Authority radio communications system is a Motorola SmartZone version 4.1 800 MHz trunked system with 12 constructed channels transmitting from five simulcast locations owned by the Authority. The five locations; three at Dulles Airport, one at National Airport, and one at Tyson’s Corner, Va., provide radio operations at all Authority property. Motorola Solutions provides Tier III support for the trunked radio system infrastructure and a portion of the subscriber radios. Offeror personnel will provide all other required support.

C. The Department operates multiple, smaller 800 MHz trunked and conventional systems and small area VHF and UHF conventional radio systems to provide intra and inter-operational communications to special user groups. These system resources also provide backup communications for primary 800 MHz system users.

D. The Authority is implementing three separate 700 MHz six-channel public safety trunking systems across the airports. These channels are expected to be integrated into an Authority ‘Next
The prospective contractor will be expected to maintain these systems.

E. The Department operates an extensive 800 MHz Supplemental Radiating System (SRS) that is manufactured, designed, and supported by a third party and not the LMRS vendor supporting the 800 MHz radio system infrastructure (Motorola). The SRS uses signal amplifiers and signal-radiating antenna cable throughout the airports to capture and retransmit the “outdoor” 800 MHz trunked radio system to all users operating inside the buildings and tunnels at both airports. This system covers in excess of 552 million square feet and will be maintained by the prospective Contractor.

F. In addition to the primary 800 MHz radio system, the Authority operates separate 800 MHz “backup” systems for use when the primary 800 MHz system is unavailable. The Authority maintains multiple radio resources to enable it to interoperate with federal and local public safety partners that do not operate on 800 MHz, but are identified as operationally necessary. Together, the 800 MHz trunked radio system, the SRS, and the backup systems provide mission-critical radio communications for all Authority users, including:

1. Authority Police Department
2. Authority Fire/EMS Department
3. Airport Operations Departments
4. Airport Engineering and Maintenance Departments
5. Authority Headquarters Departments
6. Office of Engineering
7. Dulles Toll Road Department

G. The Authority’s Office of Public Safety participates in Northern Virginia and National Capital Region (NCR) mutual aid regional response agreements. These agreements require radio communications for effective emergency coordination. Authority Police and Fire/EMS (public safety) units responding to events off Authority property coordinate with adjacent public safety responders via radio and public safety first responders called to the airports use the Authority’s 800 MHz radio system to coordinate events on airport property. All 800 MHz radio system users within the NCR are equipped to communicate on the Authority’s current 800 MHz radio system and the Authority radio equipment is configured to communicate on most other systems throughout the National Capital Region (see Attachment N).

H. In addition to the system’s primary radio users and 800 MHz adjacent government users, other agencies communicate with Authority public safety on a regular basis to fulfill their mission-critical functions. A partial list of users includes the:

1. Transportation Security Administration (TSA)
2. Federal Bureau of Investigation (FBI)
3. Drug Enforcement Administration (DEA)
4. Customs and Border Protection (CBP)
5. U.S. Secret Service
6. Federal Air Marshal Service
7. U.S. Marshal Service
8. Virginia State Police (VSP)
9. Immigration and Customs Enforcement

I. The Authority is currently engaged in rebanding the 800 MHz trunked system. Rebanding is a nationwide process initiated by the FCC to mitigate interference caused by the Sprint/Nextel wideband/broadband network with adjacent public safety systems using the 800 MHz interleaved band,
which covers frequencies between 854 MHz and 861 MHz. The rebanding process is complex and requires careful planning and coordination with adjacent jurisdictions to assure emergency response communication capability remain operational throughout the process.

J. Currently, there are 3000 800 MHz, VHF, UHF, and HF radio subscriber units in use at Dulles Airport, National Airport, and on the Dulles Access and Toll Roads.

K. Current Staff - To accomplish this mission, stated goals, and requirements, the Department has sixteen (16) full-time Authority and Contractor staff and three key support contractors (e.g. the manufacturer of the primary radio communication systems, provides core technical support for the fixed station equipment and a portion of the radio subscriber equipment) that support Radio Network Operations Center (Hanger 5), National Airport, and Dulles Airport. The Chart at Appendix B provides a break out of the functions supported by the current contractor staff.

The Authority is committed to safety and excellence and strives to improve efficiency, responsiveness, and customer orientation.
SECTION III - SCOPE OF WORK

01 OVERVIEW OF SERVICES

The primary responsibility of the Contractor is to provide qualified personnel in support of the Department Mission in the following areas:

A. Radio Network Management
   1. Operate and Maintain the 800 MHz Simulcast Trunked Radio System and HF, UHF, VHF and 800 MHz Conventional Radio Systems. Tier 1/2/3 support to unsupported subscriber radios.
   2. Operation and Maintenance (Tier I, II, III, and IV) the 700 MHz Simulcast Trunked Radio System.
   3. Operation and Maintenance (Tier I/II) of the 800 MHz Trunked Radio Systems
   4. Radio Network Operations Center (RNOC) Operation and Maintenance
   5. Public Safety Communication Center Support
   6. Radio System Engineering
   7. Conduct Interference Management and Field Survey Activities.
   8. Local and Wide Area Engineering, Operation and Management
   9. Provide Radio User Field Support to Include Field Radio Programming
   10. Operate and Maintain Authority Fleet Mapping and Talk Groups.
   13. Acquire and Integrate Communications and Public Safety Special Purpose Equipment.
   15. Provide Radio and Telephone Recording and Reporting Services.
   17. Maintain computer servers, terminals, configurations and backups
   18. Maintain the MCM Asset Management & Public Safety Radio ID System

B. Mutual Aid and Interoperability Operations

C. Radio User Assistance Operations at Nation Airport, Dulles Airport, Dulles Toll and Access Roads to include user level training in the use of Authority radios.

D. Project Management

E. Radio System-Network Support Services
   1. Contract Administration and Budget
   2. Maintenance and Material Management

F. Radio Systems Network Security

The Contractor shall be required to provide qualified personnel to carry out functions associated with the operation and maintenance of the Authority's radios systems as specified in this RFP. In addition to operations and maintenance, the Contractor shall provide support for on-going and future radio/wireless projects initiated by the Authority. These projects will provide as-needed, upgrades and technology refreshment to the Authority radio environment.

The Authority will retain ownership of all hardware and software. The Authority will not purchase or lease hardware, software, equipment, or supplies from the Contractor under this contract except as specifically
described under Supplemental Repair Services. The Authority does not intend to transfer any Authority employees to the Contractor.

The scope of the contract resulting from this RFP is divided into three areas:

1. Transition Services to coordinate a ninety day transition of operations and support of the radio systems environment from the Authority to the Contractor.
2. Base Services for the on-going support of the Authority’s wireless and radio systems environment. This will include support of the Department’s mission areas cited above for the current and future Authority’s wireless and radio systems environment.
3. Supplemental Services assigned to the Contractor during the course of the contract that are not included in the scope of Base Services.

All services rendered by the Contractor will be in compliance with the Authority’s Information Security Standard (Appendix G). Examples of the standards that the Contractor will be required to comply with can be found in Appendix H and Appendix I.

During emergencies (e.g. snow storms, major power outages) all Base Services personnel are subject to recall.

02 TRANSITION SERVICES

To support a successful transition to the Base Services period, the Authority has specified a ninety day transition period for the Contractor to:

A **Provide Non-Disclosure Agreements**

The Contractor shall provide to the COTR an Authority approved Non-Disclosure Agreement for each and every consultant who provides services to the Authority. The Contractor shall also maintain a copy of every Non-Disclosure Agreement provided on-site.

B **Update, Deliver, and Implement a Transition Plan**

The Contractor shall develop and submit a transition plan with a Time Dependency Diagram showing tasks, milestones, milestone dates, and deliverables that will be accomplished during the transition period. The transition plan submitted with the proposal can be updated to add additional tasks, subtasks, and deliverables to accomplish a successful transition and shall be delivered to the Authority two weeks after contract award. The plan shall include a detailed description of transition activities for all activities required by section III.2. This updated plan shall not result in a change to the contract.

C **Present Qualified Candidates**

Except for the Senior Project Manager and Communications Analyst positions, all proposed Base Services personnel/consultants shall pass a test of essential knowledge and skills that will be administered by the COTR before these persons are permitted to work on Authority equipment under this Contract.

For the transition period, the COTR will schedule the initial set of tests to occur during the first 10 days of the transition period. At other times, the COTR will schedule testing of proposed replacement personnel/consultants within 5 days after written notice from the Contractor stating the name, qualifications of the person, and position for which the person is to be tested.
The Contractor shall promptly submit other persons for testing should any of the initially proposed persons fail the test. All transition period testing is to be completed within the first 30 days of the transition period.

The following is an example of the testing to be required:

For the Radio Maintenance Technician category, each candidate shall:

1. Demonstrate Motorola Customer Programming Software (CPS) Development and Radio Programming Skills (Element 1). The applicant will be provided with raw data and programming tools and will be asked to develop a full function trunked radio template. The applicant will use this file to provide a functioning portable (subscriber) radio. The successful applicant will go on to Element 2.

2. Demonstrate Microsoft Excel Spreadsheet Skills (Element 2). The applicant will be provided with raw data and a sample spreadsheet with multiple data members and fields and will be asked to develop and construct a duplicate Excel spreadsheet. The successful applicant will go on to Element 3.

3. Demonstrate technical knowledge through a written examination (Element 3). The applicant will be given a 50 question test to gauge a level of knowledge necessary for the position. Twenty-five (25) of the questions will concern general electronics and twenty-five (25) questions will concern trunked or conventional radio operations/systems.

D Collect and Document the Current Radio Network Environment

The Contractor will undertake a comprehensive review of the Authority’s wireless and radio systems environment. The purpose of this task is to permit the Contractor to collect and/or develop the information and documentation necessary to support successful management, operation, and maintenance of the Authority Radio Network infrastructure to include current supporting systems. To accomplish this task the Contractor shall:

1. Survey all Department sites.
2. Survey and Document all Authority Radio Systems. Use photographs to support describing each system. The contractor shall prepare system diagrams detailing the current systems including network devices and base station locations. The specific information to be displayed on the systems diagram shall be coordinated with and approved by the COTR.
3. Document automated systems (hardware, software), to include location, purpose, version numbers, licensing/warranty information/status and configurations.

E Review Operating Processes and Procedures

The Contractor will review current Authority, Office, and Department procedures and develop and submit to the COTR a recommended procedures manual for review. The Contractor is expected to draw upon the existing Authority procedures and its own existing documentation to tailor documented operating procedures for Authority use for the support areas covered by the SOW. Documented operating procedures will be updated annually and submitted for Authority approval.

F Develop and Implement Contract Performance Metrics

The Contractor shall develop and submit performance standards to the COTR for review and approval. These performance standards shall establish the performance goals and objectives for the Contractor staff. The Contractor shall propose performance standards that can be collected efficiently and
accurately from available data. The Contractor shall also propose a format for submitting performance standard scores to the COTR for review. The Authority anticipates monthly submission of performance standard scores.

G  Radio Safety Training

The Contractor will provide Radio Exposure training that meets or exceeds OSHA/FCC requirements to all contractor staff within 90 days of contract start. Full Training or an FCC/OSHA acceptable refresher class will be supplied each successive year for all Contract employees who are/may be exposed to high-level radio frequency fields. Regulations mandate workers working in Radio Frequency environments receive annual training on Radio Frequency (RF) exposure in the workplace. On-line or class courses are available to those who work on rooftops and/or near radio tower installations. Training generally covers the Maximum Permissible Exposure (MPE) ANSI C-95 standard, regulations covering workers and the general public, power density, antenna types and personal protective equipment (PPE).

H  Prepare Required Reports

The Contractor shall submit weekly status reports to the COTR during the transition period specifying progress to date on the transition plan, problems encountered and resolutions, planned activities for the upcoming week, and summarizing hours expended by labor category. Contractor timesheet shall also be submitted detailing time expended and work accomplished.

03  BASE SERVICES

Base Services include the entire range of technical and administrative support services required on an on-going basis to support the Authority’s Radio Network environment. The Base Services period will commence immediately following the ninety day Transition Services period. The Authority’s radio network environment should be secure, reliable, responsive, transparent and easily accessible to authorized users at all times. When components fail, trained personnel using consistent procedures and best practices should preserve the integrity of system, restore services, and minimize the impact on users.

The required technical and administrative services that are included in Base Services are listed in the following sections and more fully described in Appendix E. The Department’s technical administrative environment is dynamic, and all guidelines are not predetermined. Therefore, close coordination with the COTR is essential.

All personnel shall be experienced and fully qualified to perform all required or reasonably anticipated services within the scope of their area of responsibility. Contract employees are subject to prior review and verification of credentials for experience, education and certifications. They are further subject to testing for knowledge or proficiency as part of contractor evaluation and incumbent employee approval.

A  Positions Required

The below list provides a high level description of the positions required. Additional information can be found in Appendix D (Labor Categories and Descriptions), and Appendix E (Contract Position Descriptions).

1. Senior Project Manager

The Contractor shall provide one (1) Senior Project Manager to support strategic planning as well as budgeting and management of vendors and project contractors for the Wireless and Radio Systems Department, MA-630. The Contractor’s incumbent will make day-to-day
decisions and provide leadership to other contractors concerning the management of projects within guidelines provided by the Department Manager

2. **Radio and Wireless Technical Services Coordinator**

   The Contractor shall provide one (1) Radio and Wireless Technical Services Coordinators to support and accomplish the technical administrative activities of the Wireless and Radio Systems Department, MA-630. The Contractor's incumbent will make day-to-day decisions and take actions concerning the execution of work and orderly administration of activities within guidelines provided by the Department Manager.

3. **Senior Radio Engineer**

   The Contractor shall provide one (1) Senior Radio Engineer to act as technical lead for maintenance (7x24) and improvement of land mobile radio communications systems for the Wireless and Radio Systems Department, MA-630. The Contractor's incumbent will make day-to-day decisions, provide technical guidance to other contract personnel, and take actions concerning the operation and enhancement to radio systems infrastructure within guidelines provided and plans approved by the Department Manager.

4. **Communications Analyst**

   The Contractor shall provide one (1) Communications Analyst to act as project manager for the Authority’s 800 MHz rebanding project and other similar or related activities for the Wireless and Radio Systems Department, MA-630. The Contractor’s incumbent will make day-to-day decisions and take actions concerning the rebanding project within guidelines provided and plans approved by the Department Manager, as well as executed contracts.

   Note: The Communications Analyst position will be needed as a Base Services position only during the initial and first option year of the contract. After that, it shall be treated as a Supplemental Consulting Services Position.

5. **Senior Network Engineer**

   The Contractor shall provide one (1) Senior Network Engineer to provide ongoing LAN-WAN support (7x24) for the Authority's radio networks and users. The Contractor's incumbent will make day-to-day decisions and take actions concerning the development, operation and maintenance of networks supporting radio systems, within guidelines provided by the Authority. This is a key/sensitive security position.

6. **Supplemental Radiating System Field Engineer**

   The Contractor shall provide one (1) Supplemental Radiating System (SRS) Field Engineer to provide Maintenance/Support (7x24) to the Authority's extensive 800 MHz ‘In Building’ extension of the Public Safety trunked radio system. The Contractor's incumbent will make day-to-day decisions and take actions concerning the operation, maintenance, and expansion of the SRS and underlying network equipment within guidelines provided by the Authority. This is a key/sensitive security position.
7. **Radio Frequency Engineering Planner**

The Contractor shall provide one (1) Radio Frequency Engineering Planner to support the Wireless and Radio Systems Department, MA-630 in strategic planning, to represent the Authority at the regular (FCC, Region 20 Planning and Metro Washington Council of Governments meetings, to identify federal grant funding and to perform evaluations of (QC) of contracted technical support services. The Contractor’s incumbent will make day-to-day decisions and represent the Authority within guidelines provided by the Department Manager.

8. **System Analyst**

The Contractor shall provide one (1) System Analyst to provide ongoing support and training for the Authority's tactical and emergency communications activities, provide 24x7 radio system technical support to the Authority Public Safety Communications Center and to coordinate Interoperable radio encryption “keys” with Authority federal partners. The Contractor's incumbent will make day-to-day decisions and take actions to plan, train and execute tactical plans and deploy communications assets within guidelines provided by the Authority. This is a key/sensitive security position.

9. **Senior Radio (Infrastructure) and Networking Technologist**

The Contractor shall provide one (1) Senior Radio and Networking Technologist to Design, Implement and Fully Support (7x24) all computer-based systems supporting the radio system, radio site security and ‘real time’ critical radio infrastructure alarm environment. The Contractor’s incumbent will make day-to-day decisions and take actions concerning the development, operation and maintenance of these multiple radio and monitoring networks within guidelines provided by the Authority. This is a key/sensitive security position.

10. **Field Radio Support Technician/Radio Communications Integration Technician**

The Contractor shall provide two (2) Field Radio Support Technician/Radio Communications Integration Technician to provide custom installations and maintenance of mobile radios, mobile computers, specialized equipment and emergency lighting to the Authority motor fleet. The Contractor's incumbent will make day-to-day decisions and take actions concerning the installation and maintenance of various electronic equipment in Authority vehicles within guidelines provided by the Authority.

11. **Radio Maintenance Technicians**

The Contractor shall provide two (2) Radio Maintenance Technicians to perform on-going daily support of subscriber radios, radio infrastructure and antenna systems. The Contractor will be expected to make day-to-day decisions and take actions concerning the operation and maintenance of radio equipment and support users within guidelines provided by the Authority.

**B Radio Technology Training Required**

Each year of the contract, the Contractor shall provide up to eighty (80) hours of radio/wireless systems specific training to Contract employees identified by the COTR.
04 SUPPLEMENTAL SERVICES

A Supplemental Repair Services

The Authority Radio Systems are comprised of a large number of diverse and customized components. While the Authority strives to maintain an adequate inventory of spare parts, there may arise the need for an emergency acquisition of a part or parts needed to restore service.

In such an instance, the needed part(s) may be obtained from the contractor through the issuance of a call order.

B Supplemental Construction Services

The Contractor will be responsible for and provide oversight to subcontractors selected to provide labor, equipment, and materials to meet supplemental construction support tasks. The work to be performed will be of a temporary nature, and may require a diversity of skills suitable to a variety of Telecommunications functions, including but not limited to:

- Large installations or equipment moves
- Construction projects including the laying of conduit and cable

The work required throughout the duration of any task will vary with each requirement depending upon the scope of the work to be performed. Specific work to be performed will be included in a statement of work for the individual requirement.

The Contractor will be required to submit a specific technical and price proposal for all Airports Authority requests for Supplemental Construction Support Services. The proposals will include:

- Proposed prices with sufficient breakdown to allow a thorough analysis, including indirect and direct rates
- Technical approach to performance of services
- Personnel qualifications
- Subcontractor mark-ups

The Contractor will be responsible for providing Supervision and Quality Assurance (i.e. testing) on all supplemental construction activities.

Products and services provided must be obtained through processes that comply with the Authority’s Procurement Policies. This includes using Authority approved Local Disadvantaged Business Enterprise (LDBE) vendor lists provided by the Business Office.

C Supplemental Consulting Services

The Authority’s Telecommunications workload is variable and unexpected demands sometimes arise. The Contractor will be responsible for providing competent radio communications specialists to meet variable demands in workload. The work to be performed will be of a temporary nature, and could require a diversity of skills suitable to a variety of radio communications functions, including:

1. Large system installations or equipment moves
2. Integration of new technology
3. Special studies and planning projects
4. Special software application, modification or upgrade
5. Other work assigned to the Wireless and Radio Systems Department

D Contract Services Call Order

Supplemental Services shall be requested and approved in advance by the COTR using the “Contract Services Call Order” form shown in Appendix M. The Call Order will contain a detailed description of the services that are required from the Contractor. The Contractor shall provide the COTR a detailed cost estimate including an itemized breakdown for all labor, parts and materials and shipping as well as a schedule with critical milestones for completing the work to be listed on the Call Order. Additionally, a specific technical proposal shall be submitted for all Authority requests for Supplemental Consulting Services. The proposals will include:

1. Proposed prices with sufficient breakdown to allow a thorough analysis including rates and hours per task to be performed
2. Technical approach to perform services
3. Personnel qualifications

Labor rates included on the contract price schedule (Supplemental Services) for the contract will be used in preparing these estimates. Both the cost breakdown and schedule shall be made part of the Call Order. The Contractor shall not proceed with any work described in such Call Orders until authorized in writing by the COTR.

05 CONTRACT ADMINISTRATION

A Location of Performance

The Contractor will provide the support services identified in this SOW to all Authority locations. Current locations are Washington Dulles International Airport, and Ronald Reagan Washington National Airport, Dulles Access Road, and the Tyson’s Corner Tower Site.

B Required Hours of Operation

Hours of operation currently required are documented in the chart below:

<table>
<thead>
<tr>
<th>Contract Position or Functional Area</th>
<th>Hours of Availability</th>
<th>Normal Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Senior Project Manager</td>
<td>8:30 AM to 5:30 PM</td>
<td>8:30 AM to 5:30 PM</td>
</tr>
<tr>
<td>2 Radio &amp; Wireless Technical Service Coordinator</td>
<td>8:30 AM to 5:30 PM</td>
<td>8:30 AM to 5:30 PM</td>
</tr>
<tr>
<td>3 Senior Radio Engineer</td>
<td>24 hours per day</td>
<td>8:30 AM to 5:30 PM</td>
</tr>
<tr>
<td>4 Communications Analyst</td>
<td>Flexible Scheduling</td>
<td>8:30 AM to 5:30 PM</td>
</tr>
<tr>
<td>5 Senior Network Engineer</td>
<td>24 hours per day</td>
<td>8:30 AM to 5:30 PM</td>
</tr>
<tr>
<td>6 SRS Field Engineer</td>
<td>24 hours per day</td>
<td>8:30 AM to 5:30 PM</td>
</tr>
<tr>
<td>7 Radio Frequency Engineering Planner</td>
<td>Flexible Scheduling</td>
<td>8:30 AM to 5:30 PM</td>
</tr>
<tr>
<td>8 System Analyst</td>
<td>24 hours per day</td>
<td>8:30 AM to 5:30 PM</td>
</tr>
<tr>
<td>9 Senior Radio and Networking Technologist</td>
<td>Flexible Scheduling</td>
<td>2:30 PM to 11:30 PM</td>
</tr>
<tr>
<td>10 Field Radio Support Technician/ Radio Communications Integration Technician (2)</td>
<td>Flexible Scheduling</td>
<td>8:30 AM to 5:30 PM</td>
</tr>
<tr>
<td>11 Radio Maintenance Technician (2)</td>
<td>24 hours per day</td>
<td>8:30 AM to 5:30 PM</td>
</tr>
</tbody>
</table>

During the hours that the Department is not staffed, the Authority requires the ability to contact and notify Contractor Personnel of urgent or emergency situations (by wireless telephone, messaging device, or service). The Contractor will return messages or pages within one hour during off-hours. The Contractor will be required to arrive on-site within three hours notice, although the Contractor may
propose a shorter period. Overtime shall be at the hourly rate proposed by the Contractor for a normal 8 hour work day. Contractor employees may be required to work adjusted schedules outside of normal working hours for episodic, or pre-planned outages or work efforts to minimize impact to users.

C Other Support Contracts

The Contractor will coordinate support and maintenance activities with other Authority contractors on site. This contract will involve oversight but not supervision of other support contractors.

The Contractor is required to review existing Authority support contracts as they come up for renewal. The Contractor will evaluate requirements and existing support activities and make recommendations, where necessary, to achieve optimum system performance through the support contract.

D Contractor Provided Resources – Base Services

The Contractor is expected to provide each person assigned to the contract with a cellular telephone and service that meets the Authority’s technical, operational and procedural requirements. Smart-phones will be configured to the Authority’s standards for connection to the Authority e-mail system (see Appendix L). Smart-phones will be used to coordination services, access the Authority Work Order Systems, report and receive automated alarms and for contact ‘after-hours.’

The Contractor shall supply wireless carrier-based (wide area) broadband equipment and service to select COTR-identified contractor personnel to permit remote access, monitoring and Control of radio system network resources. Additionally, the Contractor will also provide normal tools of the trade for contract staff assigned to the Authority as shown in Appendix F.

The Contractor shall:

1. Pay fees necessary for employee badging and security, as outlined below:

   A. Ronald Reagan Washington National Airport. ID Badges are issued for $50/year per badge.
   B. Washington Dulles International Airport. ID Badges are issued for $50/year, per badge
   C. There is an escalating fee to replace a lost badge. The first time fee is $50.

   Note: The Airports Authority can adjust all fees as needed. ID Badges expire on the last day of the birth month of the holder. In addition to the annual badge fee, there is a one-time fee of $27 for a Fingerprint based Criminal History Records Check (includes fingerprinting) and $11 for a one time only Security Threat Assessment.

   In order to receive an Airport issued airport operations area or a sterile area identification Badge, each person must be fingerprinted at their respective airport (National or Dulles Airport Pass & ID Office); successfully complete an FBI criminal history records check (CHRC) and; pass a TSA Security Threat Assessment (STA). Additional fingerprinting (no more than one year old) is required and conducted by Customs and Border Control (CBP) for those who need access to customs areas and to obtain a U.S. Customs seal on the identification badge.

   Due to the critical and sensitive nature of the Authority radio systems, additional background checks and driving record reviews may be conducted.
2. Pay fees necessary for employee for parking, where applicable, as outlined below:
   A. **Ronald Reagan Washington National Airport.** Parking available in employee parking lot for $95.00/year.
   B. **Washington Dulles International Airport.** Parking available in employee parking lot for $350.00/year.
   C. Note: Parking fees are adjusted each year in October. The parking fees cover the period October 1 through September 30. The fees specified above will remain in effect until September 30, 2012.

3. Provide a minimum of 40 hours technical radio related training to each contractor each year as approved by the COTR.

**E Authority Provided Resources**

The Authority will provide all network and workstation hardware and software required by the Authority’s system. All procurements for Authority systems will be made by the CO, with recommendation and technical assistance from the COTR. The Authority will retain ownership, leases or licensure of all hardware, software, and data.

The Contractor will be responsible for the normal care and security of all Authority property issued during the contract term. A property inventory of all issued assets will be conducted on the first and last day of the contract term to determine Contractor accountability of Authority property. The Contractor will be responsible for conducting an inventory of Authority issued property semi annually including reconciliation to the prior inventory. The Authority will conduct unscheduled property inventories during the Contract term. See Appendix J for additional information.

The following resources will be provided by the Authority:

1. Adequate work space
2. Access to work sites (As necessary and Authorized for Field Work)
3. Workstations for on-site Contractor personnel.
4. Equipment and access to Authority-owned communications systems necessary for official, routine contact with Contractor personnel, or as necessary to support routine work efforts and troubleshooting.
5. Telephone service with voice mail
6. Special purpose computers
7. Internet access (for the download of software patches and related items)
8. Authority E-Mail Access for Official Authority Communications
9. Authority Radio and Wireless Communications Systems
10. Daily operating supplies, materials, and hardware necessary to effect installation or repair of equipment.

**F Reporting Requirements**

1. Monthly status reports - After the Transition Services period is completed, the Contractor will submit a monthly report to the CO and COTR that describes the overall status of the contract and the Authority network and systems. This report will follow a format agreed to by the Authority and the Contractor. The format of the report is expected to change from time to time. Initially, the report is expected to contain the following sections:
A. Overview
   - Accomplishments, Planned Activities, Summary of Performance Metrics, and Issues
   - Tracking of performance and other Authority identified metrics

B. Personnel
   - A list of all Base Services positions and assigned personnel

C. Base Services
   - Cost summary
   - Activities accomplished
   - Usage Statistics/Measures

D. Supplemental Services
   - Supplemental Repair Services review
   - Supplemental Consulting Services Project Summaries

E. Other Information pertinent to performance
   - LDBE (Local Disadvantaged Business Entity) tracking

2. Program Management Reviews and Planning Meetings - The Contractor will coordinate monthly Program Management Reviews with the COTR and the Vice President, Information and Telecommunication Systems. The purpose of these reviews will be to review the monthly status report and discuss high-level management issues and plans with Contractor management personnel. The Contractor’s Program Manager and appropriate management team personnel will be present at these reviews. The Contractor will maintain and publish minutes of these meetings.

3. Weekly Status Report - The format for these reports shall be provided by the Department Manager within one week after start of Contract.

4. Contractor Time Sheet – Contractor employees must submit a completed time sheet in triplicate every Friday for the approval and signature of the COTR (Contracting Officer’s Technical Representative). A copy of each approved and signed time sheet must be left with the COTR, and a copy must accompany monthly invoices submitted for payment to the Authority by the contractor. Note: This is a fixed price contract, not time and material.

G Key Personnel

All Base Services personnel proposed by the Contractor will be considered for the purposes of award and contract administration as “key personnel.” The Contractor shall identify and submit resumes for these key personnel positions in their proposals, as described in the Instructions to Offerors.

The Contractor shall use its best efforts to notify the CO and COTR within 30 days prior to required approval to reassign any key personnel during the life of the contract. The CO reserves the right to approve replacement personnel and shall require retention of key personnel until a suitable replacement is found.

The Contractor shall state the commitment of key management personnel to the Airports Authority contract by providing the percentage of full-time work devoted to this contract.
The Airports Authority expects that personnel designated as “key personnel” are current employees of the Contractor/Subcontractor firm, unless notified otherwise.

H **Removal of Staff**

The Authority shall have the unqualified right to require, with or without cause, the offeror to remove, replace, or change the assignment of any vendor personnel assigned to the Contract. Should the Authority at any time request that any vendor personnel be changed, the vendor agrees to do so within the time frame specified in the Authority’s written request.
SECTION IV - DELIVERABLES

01 PLANS AND OTHER DOCUMENTS

The below documents are due at the completion of the transition period unless noted otherwise.

A. Non-Disclosure Agreements
B. Updated Transition Plan – No later than two weeks after Contract Award.
C. Documentation of Authority Radio Systems
D. Documentation of Authority automated systems (hardware, software) used MA-30
E. Recommended Procedures Manual
F. Recommended Performance Standards/Metrics

02 PERSONNEL

A. Senior Project Manager
B. Radio & Wireless Technical Services Coordinator
C. Senior Radio Engineer
D. Communications Analyst
E. Senior Network Engineer
F. Supplemental Radiating System Field Engineer
G. Radio Frequency Engineering Planner
H. System Analyst
I. Senior Radio and Networking Technologist
J. Field Radio Support Technician/Radio Communications Integration Technician (2)
K. Radio Maintenance Technician (2)

03 PERIODIC REPORTS

A. Weekly Reports (Close of business each Thursday)
B. Weekly Time Sheets (Close of business each Friday)
C. Monthly Reports (As Established by the Department Manager)
D. Monthly Meeting Minutes
SECTION V - APPENDICES
APPENDIX A

ORGANIZATION CHART MA-630
APPENDIX B

CHART OF CURRENT STAFF FUNCTIONS
APPENDIX B - Detailed Functional Groupings

Wireless and Radio Systems Department
Office for Information and Telecommunications Systems

Radio Network Management
  - Radio Network Operations Center (RNOC)
    - CCC Support
  - Radio Systems Engineering
  - Surveys and Interference Mitigation
  - LAN – WAN Engineering
  - Radio System Programming & Fleet Mapping

Mutual Aid and Interoperability Operations

User Assistance Operations
  - IAD
  - DCA
  - Training

Projects

Radio System-Network Support Services
  - Contract Administration and Budget
  - Maintenance and Material Management

Radio Systems Security

MA-630 Manager
  - Administration
Functional Group

MA-630 Manager

Functions Included

- Procurement Management (74)
  - Prepare Purchase Requests
  - Invoice Reconciliation and Approvals
- Escort Services - Non Technical (77)
- Reporting (78)
- Space Management (79)
- Personnel Actions, Time Reporting (80)
- Safety (85)
Operate and Maintain a Radio Network Operations Center (RDOC) (03)
- Operate the RDOC – 6 AM – 10 PM
- Technical Support to the PS CCC
- Fault and Problem Identification – Resolution (04)
- Detect - Monitor Alarms (05)
- Trouble Shoot – Diagnose (06)
- Isolate the Problem (07)
- Corrective Actions (08)
- Technical Administration (09)
- Performance Management (11)
- Monitor Performance Metrics (12)
- Optimize, Adjust, Balance (FCC allowable Tolerances)(13)
- Implement Backups (19)
- Radio Computer Server Operation and Management (20)
- Technical Documentation (14)
- Performance Management (11)
- Local Area Network-Wide Area Network Operation/Maintenance (21)
- Control and Assign Internet Protocol (IP) Addresses (18)
- Growth Management (27)
- Authority Fleet Map (23)
- Maintain Radio System, System Component, Radio Configurations (24)
- Performance Management (11)
- Fail Soft Planning, Development, and Programming (17)
<table>
<thead>
<tr>
<th>Functional Group</th>
<th>Functions Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual Aid and Interoperability Operations (1)</td>
<td></td>
</tr>
</tbody>
</table>

- Authority Point-of-Contact (POC) for Radio and Wireless Mutual Aid and Interoperability Technology (1).
  - Conduct liaison with all of the neighboring jurisdictions
  - Exchange radio specific, detailed radio and programming data to enable mutual aid communications.
  - Participate in interoperability activities at the Federal (Department of Homeland Security) and state levels.
  - Support Implementation of the National Incident Management System (NIMS).
  - Attend “interoperability” planning meetings at the Federal (Department of Homeland Security) and state levels.
  - Negotiate technically feasible interoperability standards.
- Technical Integration and Interface Specifications (30)
**Functions Included**

- **User Assistance Operations (43)**
  - User Assistance Actions (44)
  - Conduct User Satisfaction Surveys (45)
  - Daily Site Checks (47)
  - User Support Services – Field (50)
    - First Response to Requests – Problems (48)
    - Performs Analysis, Troubleshooting, Solution Delivery (49)
    - Conducts Preventive Maintenance Services (51)
    - Radio Support - Installs (52)
    - Radio Support - Implements Radio Templates (53)
    - Radio Support - Program and Configure (54)
    - Implement Radio Programming (field activity) (35)
  - Conduct 1st Tier Maintenance on Radio Resources - MA-630 Staff (66)
  - Roof Mounted Antennas - Installs, Replaces, Repairs (56)
  - Radio Support - Install Headset-Intercoms Public Safety Vehicles (55)
  - Building Radiating Systems – Install, Replace, Repair, Tier 1 (57)

- **IAD**
  - Training (46)

- **DCA**

- **Training**
Projects (81)

Radio System-Network Support Services

Contract Administration and Budget

Maintenance (64) and Material (75) Management

Radio Systems Security (36)

Functions Included

- Department Five Year Plan
- Strategic Initiatives
- Prepare Statements of Work
- Proposal Evaluations
- Project Management
  - Oversee, develop, and/or manage, multiple projects
  - Assist Authority Management In Forecasting Requirements
  - Develop clear project goals and plans
  - Scope Development
  - Identify And Describe Project Tasks
  - Prepare Cost Estimates
  - Manage Resources To Perform Assigned Projects
  - Conduct and/or coordinate status meetings and performance reviews
  - Oversees project performance including:
    - Cost, schedule, deliverables and contractual compliance.

- Budget Administration (730)
- Contract Administration (58)
  - Prepare Solicitation Documents (59)
  - Manage Contracts (60)
  - Escort Services for Un-badges Contractor Technicians (61)
  - Coordination (access to facilities, time, parking) (62)
  - Quality Review of Work Performed (63)

- Security Policy, Procedures, and Plans (37)
- Access Control to Physical Space (38)
- Encryption Management (40)
- Virus Control and Protections (41)
- Control and Operate the Zetron Pager System (42)

- Security Policy, Procedures, and Plans (37)
- Access Control to Physical Space (38)
- Encryption Management (40)
- Virus Control and Protections (41)
- Control and Operate the Zetron Pager System (42)

- Maintain Repair Record (69)
- Calibrates Test Equipment (70)
- Battery Maintenance and Replacement (71)
- Conducts Periodic Inventory Of Assets and Spare Parts (76)
- Materials Management (76)
  - Request Assets, Spare Parts, and Supplies
  - Receive and Control Assets
  - Store Spare Parts and Supplies
  - Maintain Inventory Records
  - Receive - Issue

Radio System and Network Maintenance Management (64)

- Maintenance Planning - PM Services (65)
- Conduct 2nd Tier Maintenance – Contractor (67)
- Conduct 3rd Tier Maintenance – Contractor (68)
- Building Radiating Systems – Install, Replace, Repair, (Tier 2, 3) (57)
- Maintain Repair Record (69)
- Calibrates Test Equipment (70)
- Battery Maintenance and Replacement (71)
- Conducts Periodic Inventory Of Assets and Spare Parts (76)

- Request Assets, Spare Parts, and Supplies
- Receive and Control Assets
- Store Spare Parts and Supplies
- Maintain Inventory Records
- Receive - Issue
APPENDIX C

EQUIPMENT & SYSTEMS LIST
### Appendix C – Equipment & Systems List

<table>
<thead>
<tr>
<th>Site</th>
<th>Equipment Locations</th>
<th>Facility</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCA</td>
<td>Hangar 5, 1st Floor</td>
<td>MA-630 System Management Offices</td>
<td>Sys Mon Point/Alarm Displays</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MA-630 Technical Services Offices</td>
<td>Sys Mon Displays</td>
</tr>
<tr>
<td>DCA</td>
<td>Hangar 5, 1st Floor</td>
<td>Radio-Network Operations Center (DCA-RNOC) and Interoperability</td>
<td>Sys Mon Point/Alarm Displays</td>
</tr>
<tr>
<td>DCA</td>
<td>Hangar 5, 3rd Floor</td>
<td>800 MHz Radio Room, Critical Parts Storage</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Hangar 5, 3rd Floor</td>
<td>Backup Radio Room (BURR)</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Hangar 5 Main Radio Room (MRR)</td>
<td>SRS and 800 Prime/Remote Site</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Hangar 5, Roof</td>
<td>Antenna Farm</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>DCA “Shops” Area, Tower</td>
<td>Shelter &amp; Backup Tower</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>West Lab Building</td>
<td>Antenna Farm/ Multi Locations</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>West Lab Bldg_, Police SOU</td>
<td>Police Motor Squad Eqpt Storage</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Hangar 11, Comm (Field) Support Unit (CSU300)</td>
<td>Interop Support</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Fire Station 301</td>
<td>Authority Command Bus (CP-346)</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Fire Station 301</td>
<td>Fire Station Alerting</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Fire Station 301</td>
<td>Battalion 301 Buggy</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>BOATHOUSE</td>
<td>River Rescue Vessels</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>PSCC/EOC, Hangar 5, 2nd Floor</td>
<td>Dispatch Consoles &amp; Alarms</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Main Terminal “A”</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Terminals B,C</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Parking Garage A</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Parking Garage B/C</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Parking Garage Pedestrian Tunnel</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Boiler / Chiller Plant</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Corporate Office Building</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Baggage Belt Areas</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>Fire Station 301</td>
<td>Vehicles/Systems Supported</td>
<td></td>
</tr>
<tr>
<td>DCA</td>
<td>AIRPORT Operations Center</td>
<td>Dispatch Console (1)</td>
<td></td>
</tr>
<tr>
<td>Tyson’s</td>
<td>Intersection of RT 7 &amp; Dulles Access</td>
<td>800 System Remote Tower Site</td>
<td></td>
</tr>
<tr>
<td>Tyson’s</td>
<td>Dulles Toll Road HQ, RT 7 &amp; S</td>
<td>Vehicles/Systems Supported</td>
<td></td>
</tr>
<tr>
<td>Tyson’s</td>
<td>Dulles Transit Partners, HQ</td>
<td>Vehicles Supported</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Joint Fire/Policie (JPF) Annex</td>
<td>Interoperability, Antenna Farm</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Fire Station 302</td>
<td>Fire Station Alerting/Vehicles/Systems</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Fire Station 303</td>
<td>Fire Station Alerting/Vehicles/Systems</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Fire Station 304</td>
<td>Fire Station Alerting/Vehicles/Systems</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Shop 1 Annex</td>
<td>Radio-Network Operations Center (IAD_RNOC) and Interop Ant Farm Sys Mon Point/Alarm Displays/Systems</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Shop 1 Annex</td>
<td>Vehicle Integration/Installation Facility</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Shop 1 Annex</td>
<td>Radio Tech Services, Offices</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Shop 1 Annex</td>
<td>SRS</td>
<td>CEMS Alarm Server</td>
</tr>
<tr>
<td>IAD</td>
<td>Police Firing Range</td>
<td>BackUp Tower</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Fuel Farm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Ramp Tower Remote Site</td>
<td>SRS and Remote Site</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>VMF, South Tower</td>
<td>800 MHz Remote Site</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>ARFF, North Tower</td>
<td>800 MHz Remote Site</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>AIRPORT Operations Center</td>
<td>Dispatch Consoles (2)</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>“Old Stone House”</td>
<td>Remote Consoles for Aerotrain</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Main Terminal Aerotrain Station &amp; Tunnels</td>
<td>SRS/Systems</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>A Aerotrain Station and Tunnels</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>B Aerotrain Station &amp; Tunnels</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>C Aerotrain Station &amp; Tunnels</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>E Aerotrain Station &amp; Tunnels</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>Site</td>
<td>Equipment Locations</td>
<td>Facility</td>
<td>Comments</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------</td>
<td>----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>IAD (Old)</td>
<td>Air Traffic Control Tower (ATCT)</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD (Old)</td>
<td>Air Traffic Control Tower (ATCT)</td>
<td>Radio Interop</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Main Terminal Comm Room (B**)</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Main Terminal, Comm Room (G**)</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Main Terminal, Ground Floor, East</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Main Terminal, Ground Floor, West</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Main Terminal, Basement</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Main Terminal, Southeast Bag Basement</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Main Terminal, Z Gates &amp; Basement</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Midfield Terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Fire Station 304</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>South 800 MHz Remote Site</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Back Up Tower Site</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Live Fire Training Facility</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>North Parking Garage and Landside Pedestrian Tunnel</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Wind Shear Pole Site</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>IAD Airside Pedestrian Tunnel</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD (New)</td>
<td>Air Traffic Control Tower (ATCT)</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>West Utility Building Tunnel (WUBT)</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Vehicle Maintenance Facility (VMF)</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Smithsonian National Air and Space Museum (NASM)</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>Aviation Drive - 4 Buildings</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>IAD</td>
<td>International Arrivals Building (IAB)</td>
<td>SRS</td>
<td></td>
</tr>
<tr>
<td>RESTON</td>
<td>Reston International Center (RIC)</td>
<td>SRS tie to Fairfax County</td>
<td></td>
</tr>
</tbody>
</table>
MWAA 800 MHz Supplemental Radiating System/ Equipment Summary (as of 02/21/12):

Reagan National Airport:
30: Bi-Directional Amplifiers (BDA) + Fiber-Optic Transceivers (FOT)
20: Battery Backup Units (BBU) + UPS + Battery Extenders
72: Coverage antennas + Terminators

Washington Dulles International Airport:
139: Bi-Directional Amplifiers (BDA) + Fiber-Optic Transceivers (FOT)
72: Battery Backup Units (BBU) + UPS + Battery Extenders
454: Coverage Antennas + Terminators

134,000 Linear Feet of Installed Radiating Cable (Both Airports)

Note: Bi-Directional Antenna System Components (10% are Replaced Annually)

Manufacturers of SRS Equipment in use includes,
- AFL / Axell Wireless (UK)
- Andrew Corporation
- Kaval
- APC
- BEST

AFL/AXEll Wireless CEMS (SRS Alarm Monitoring System)
  Dell Servers (2)
  Dell Desktops (4)
  CISCO 3750G_24 (1)

This above is intended to illustrate some locations and a sampling of scope supported by the contract. "SRS" denotes the presence of components supporting the 800 MHz “In Building” Supplementary Radiating System.
### Radio LAN Equipment List

<table>
<thead>
<tr>
<th>DCA</th>
<th>LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASA</td>
<td>DCA</td>
</tr>
<tr>
<td>Cisco 2690</td>
<td>DCA</td>
</tr>
<tr>
<td>Cisco 3550-48</td>
<td>DCA</td>
</tr>
<tr>
<td>Cisco 3550-24</td>
<td>DCA</td>
</tr>
<tr>
<td>Cisco 3550-48</td>
<td>DCA</td>
</tr>
<tr>
<td><strong>Tysons Corner</strong></td>
<td></td>
</tr>
<tr>
<td>Cisco 3550-48</td>
<td>TYSONS</td>
</tr>
<tr>
<td>Cisco 2690 Router</td>
<td>TYSONS</td>
</tr>
<tr>
<td><strong>IAD</strong></td>
<td></td>
</tr>
<tr>
<td>Cisco 2811</td>
<td>IAD</td>
</tr>
<tr>
<td>Cisco 3508 Switch</td>
<td>IAD</td>
</tr>
<tr>
<td>Cisco 3550-48</td>
<td>IAD</td>
</tr>
<tr>
<td>Cisco 3550-24</td>
<td>IAD</td>
</tr>
<tr>
<td>Cisco 3550-48</td>
<td>IAD</td>
</tr>
<tr>
<td>Cisco 3750-48</td>
<td>IAD</td>
</tr>
<tr>
<td>Cisco 3550-38</td>
<td>IAD</td>
</tr>
<tr>
<td>Cisco 3750-48</td>
<td>IAD</td>
</tr>
<tr>
<td>Cisco 3650-24PS-S</td>
<td></td>
</tr>
<tr>
<td>Cisco 3750-48TS-S</td>
<td>DCA</td>
</tr>
<tr>
<td>Cisco 3750-24TS-S</td>
<td>DCA</td>
</tr>
<tr>
<td>Cisco 2851</td>
<td>DCA</td>
</tr>
<tr>
<td>Cisco 3550-48-SMI</td>
<td>DCA</td>
</tr>
<tr>
<td>Cisco 3750-48TS-S</td>
<td>DCA</td>
</tr>
<tr>
<td>Cisco 2851</td>
<td>CSU-300</td>
</tr>
<tr>
<td>Cisco 3560</td>
<td>CSU-300</td>
</tr>
</tbody>
</table>

All equipment above will be replaced during FY 2012.
SERVER / CLIENT LIST

WINS SERVER, PRIMARY
WINS SERVER, SECONDARY

MICROSOFT WSUS SERVER
RLAN NETWORK MANAGEMENT SERVER
MICROSOFT REMOTE DESKTOP MANAGEMENT SERVER

GENESIS SERVER_APPLICATION
GENESIS SERVER_DB (SQL)

GENESIS_CLIENT (2)
MCM SQL DB SERVER
MCM AP SERVER
MCM “JUMP” SERVER,
MCM “KIOSK” CLIENT (12)

CEMS SERVER_AP SERVER
CEMS (SQL) DB SERVER
CEMS “KIOSK” CLIENT (4)

SWIFT SERVER, PRIMARY A
SWIFT SERVER, SECONDARY A
SWIFT SERVER, PRIMARY B
SWIFT SERVER, SECONDARY B
SWIFT SETUP SERVER
SWIFT USER CLIENT_ (4)

CATALYST IPM SMART SERVERS (13)
CATALYST NAR SERVER (2)
CATALYST CLIENT_ (12)

SCANSTAR REMOTE MONITORING SERVER_RMA II (3)

QNAP NAS SERVER
BUFFALO TETRASTATION NAS (2)

PRIMEX CLOCK GPS_BASED NTP SERVER
SPECTRACOM GPS NETCLOCK 9129, NTP SERVER
SPECTRACOM GPS NETCLOCK 9183, NTP SERVER
SOLARWINDS ORION NPM_AP SERVER
SOLARWINDS ORION NPM_DB SERVER
SOLARWINDS ORION NPM_USER SERVER (2)
SYMANTEC END POINT PROTECTION (EPP)_APPLICATION
SYMANTEC DEEP INSIGHT_SERVER
GFI WEBMONITOR SERVER

AXIS IP CAMERA MANAGEMENT SYSTEM VIDEO_SERVER (2)
AXIS CAMERA STATION WORKSTATIONS (2)
AIRTIME_ACCUM INTERFACE APPLICATION (ATIA)
CLIENT (3)

(2) SENSAPHONE IMS-1000 INFRASTRUCTURE MONITORING SERVER

(3) RAYTHEON JPS ACU-1000__Fixed Interoperability Switch

(1) RAYTHEON JPS TPU-1000__Transportable Interoperability Switch

(1) CATCOM ICRI_Incident Commanders Radio Interoperability

(2) CADEX BATTERY MANAGEMENT SYSTEM_CLIENT/SERVER

MOTOROLA

MOTOROLA MOSCAD ALARM MANAGEMENT__SERVER
MOTOROLA MOSCAD ALARM MANAGEMENT_CLIENT (4)

MOTOROLA CENTRACOM GOLD ELITE DISPATCH_SERVER
MOTOROLA CENTRACOM GOLD ELITE_CLIENT (20)

MOTOROLA NETWORK MANAGEMENT SYSTEM_CLIENT (4)
MOTOROLA ZONE LEVEL FULLVISION SERVER (3)

MOTOROLA ZONE MANAGER DATABASE SERVER(ZMDS) (2)

MOTOROLA ZONE STATISTICS SERVER(ZSS) (2)

MOTOROLA USER CONFIGURATION SERVER (UCS) (2)

MOTOROLA TERMINAL SERVERS (2)

MOTOROLA NTP SERVER (2)
MOTOROLA ATIA_SERVER

MOTOROLA ZONE CONTROLLER 1 (NIC3)
MOTOROLA ZONE CONTROLLER 2 (NIC3)
SPECIAL USE LAPTOPS _ Field Programming, Diags, Remote System Access

- PANASONIC CF-30 (10)
- MOTOROLA ML900 (8)
- MOTOROLA ML910 (8)

TOTALS: 67 Servers (RLAN + Motorola)
         93 Clients (RLAN Desktops + Laptops + Motorola)
<table>
<thead>
<tr>
<th>Radio Count</th>
<th>Model</th>
<th>Freq Band</th>
<th>Port/Mob</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Astro Spectra Mobile</td>
<td>136-162MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>2</td>
<td>Astro Spectra Mobile</td>
<td>146-178MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>3</td>
<td>Astro Spectra Mobile</td>
<td>146-178MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>3</td>
<td>Astro Spectra Mobile</td>
<td>403-437MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>3</td>
<td>Astro Spectra Mobile</td>
<td>438-482MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>1</td>
<td>Astro Spectra Mobile</td>
<td>470-520MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>1</td>
<td>Astro Spectra Mobile</td>
<td>800MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>1</td>
<td>Astro Spectra Mobile Plus</td>
<td>800MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>1</td>
<td>Astro Spectra Mobile Plus</td>
<td>800MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>1</td>
<td>Astro Spectra Mobile Plus</td>
<td>800MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>1</td>
<td>Astro Spectra Mobile Plus</td>
<td>800MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>2</td>
<td>XTS3000 Model I</td>
<td>800MHz</td>
<td>Portable</td>
</tr>
<tr>
<td>25</td>
<td>XTS3000 Model I</td>
<td>800MHz</td>
<td>Portable</td>
</tr>
<tr>
<td>310</td>
<td>XTS3000 Model III</td>
<td>800MHz</td>
<td>Portable</td>
</tr>
<tr>
<td>61</td>
<td>XTS3000 Model III</td>
<td>800MHz</td>
<td>Portable</td>
</tr>
<tr>
<td>2</td>
<td>XTS5000 Model III</td>
<td>146-178MHz</td>
<td>Portable</td>
</tr>
<tr>
<td>3</td>
<td>XTS5000 Model III</td>
<td>380-470MHz</td>
<td>Portable</td>
</tr>
<tr>
<td>415</td>
<td>XTS5000 Model III</td>
<td>800MHz</td>
<td>Portable</td>
</tr>
<tr>
<td>15</td>
<td>XTS2500 Model 1.5</td>
<td>800MHz</td>
<td>Portable</td>
</tr>
<tr>
<td>45</td>
<td>XTS2500 Model I</td>
<td>800MHz</td>
<td>Portable</td>
</tr>
<tr>
<td>5</td>
<td>Astro Spectra Consolette</td>
<td>146-178MHz</td>
<td>Portable</td>
</tr>
<tr>
<td>2</td>
<td>Astro Spectra Consolette</td>
<td>403-437MHz</td>
<td>Portable</td>
</tr>
<tr>
<td>16</td>
<td>Astro Spectra Consolette</td>
<td>800MHz</td>
<td>Portable</td>
</tr>
<tr>
<td>19</td>
<td>Tone Remote Consolette</td>
<td>800MHz</td>
<td>Portable</td>
</tr>
<tr>
<td>8</td>
<td>Motorcycle Mobile</td>
<td>800MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>1</td>
<td>Motorcycle Mobile</td>
<td>800MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>225</td>
<td>XTL5000 O5</td>
<td>800MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>18</td>
<td>XTL5000 W3</td>
<td>800MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>39</td>
<td>XTL5000 W5</td>
<td>800MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>56</td>
<td>XTL5000 W7</td>
<td>800MHz</td>
<td>Mobile</td>
</tr>
<tr>
<td>30</td>
<td>APX6000 Mod III</td>
<td>800MHz</td>
<td>Portable</td>
</tr>
</tbody>
</table>

**Total Motorola Subscriber Radio Count:** 2231

**Note:** Legacy equipment no longer maintained by Motorola is highlighted in yellow.

(520) ICOM Model IC A-110 VHF Aeronautical mobile radios
(50) Assorted ICOM VHF Aeronautical portable radios
**Total Aeronautical radios:** 570

(18) Motorola ModelGTR-8000 700 MHz _ Astro 25 Express
(15) Motorola Quantar TS365 Stations_ Intellirepeaters
(15) Motorola Quantar TS365 Stations_ SmartNet /Astro
**Total Motorola 800 MHz Fixed-Station Equipment:** 48 Stations

(15) RELM S-Series 800 MHz Repeaters
(7) Relm Eclipse 800 MHz Repeaters
(2) Relm S-Series VHF Base Stations
**Total RELM “Backup” Fixed-Station Equipment:** 24
APPENDIX D

LABOR CATEGORIES AND DESCRIPTION
<table>
<thead>
<tr>
<th>Line #</th>
<th>Experience</th>
<th>Education</th>
<th>Substitution for education listed above (in addition to TOTAL Years required):</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>2</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>3a</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>3b</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>3c</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>3d</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>3e</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>4</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>5</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>6</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>7</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>8</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>9</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>9a</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>10</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>11a</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>12</td>
<td>Experience</td>
<td>Education</td>
<td>Substitution for education listed above (in addition to TOTAL Years required):</td>
</tr>
<tr>
<td>Line</td>
<td>Codes: &quot;R&quot; - Required  &quot;P&quot; - Preferred  &quot;X&quot; - Relevant Experience(s)</td>
<td>Senior Project Manager</td>
<td>Radio and Wireless Technical Services</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------</td>
<td>------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>15.</td>
<td>Certificate - Motorola MOSCAD Maintenance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>Certificate - Motorola MOTOMESH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>ASTRO®25 IV&amp;D</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.</td>
<td>ASTRO®25 IV&amp;D Radio System Administrator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.</td>
<td>ASTRO®25 IV&amp;D M Core Technician</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20.</td>
<td>ASTRO®25 IV&amp;D L Core Site Technician</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21.</td>
<td>ASTRO®25 IV&amp;D Conventional K Core with Configuration Manager Technician</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22.</td>
<td>ASTRO®25 IV&amp;D Repeater Site Technician</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>Functional Areas:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.</td>
<td>Develops and Coordinates Mutual Aid/Interoperability</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Conducts liaison with inter-op partners</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Exchanges data supporting mutual aid communications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Participates in Regional Interoperability Standards Development Committees</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>Develops, Conducts and Evaluates Department of Homeland Security-compliant tabletop, functional and full-scale exercises, with specific emphasis on communications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Develops After-Action Reports and Improvement Plans.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15a</td>
<td>Maintains Radio Network Operations Center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>Fault and Problem Identification - Resolution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>Detects Monitors System Alarms and Alerts _24x7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.</td>
<td>Troubleshoots - Diagnoses System and User Issues</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.</td>
<td>Isolates Problem</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20.</td>
<td>Coordinates and/or Initiates Corrective Actions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21.</td>
<td>Provides Technical Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Uses and supports network administrative systems to ensure accurate network inventory, performance indicators, and configurations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Works with the Authority stakeholders, end users, and vendors to analyze needs and problems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22.</td>
<td>Performs Field Interference Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23.</td>
<td>Monitors Performance Metrics</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Demonstrates knowledge of communications process establishment and integration.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24.</td>
<td>Optimizes, Adjusts, Balances Radio Network to FCC allowable Tolerances</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25.</td>
<td>Prepares Technical Documentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Documents Existing Wireless and Radio Data Technology.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Prepares or assists in the preparation of service record and documentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line #</td>
<td>Codes: &quot;R&quot; - Required  &quot;P&quot;- Preferred  &quot;X&quot; - Relevant Experience(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Senior Project Manager  Radio and Wireless Technical Services  Communications Analyst  Supplemental Radiating System Field  Radio Frequency Engineering Planner  Senior Radio (Infrastructure) and Networking Specialist  Field Radio Support Technician  Communications Integration Technician  Radio Maintenance Technician</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Conducts Radio Site Surveys</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>27</td>
<td>Conducts FCC Compliance Activities</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>28</td>
<td>Conducts  FailSafe Planning, Implementation and Testing</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>29</td>
<td>Controls and Assigns Internet Protocol (IP) Addresses</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>30</td>
<td>Configures, Implements, Manages Automated Data Backups</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>31</td>
<td>Installs, Configures, Operates and Manages Radio Network Computer Servers. Provides 24x365 Availability</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>32</td>
<td>Operates and Maintains Local and Wide Area Networks Provides 24x365 Availability</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>33</td>
<td>Performs Radio Network Administration</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>34</td>
<td>Designs, Prepares and Maintains 800 MHz Radio Fleet Maps</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>35</td>
<td>Maintains Radio Systems, System Components, Radio Configurations</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>36</td>
<td>Performs Frequency Management</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>37</td>
<td>Develops and Maintains Internal and External Radio Guidelines, Procedures, and Standards 1. Is aware of standards and regulatory requirements related to assigned tasks. Develops policies and procedures to support the Department Mission and ensures adherence to standards and regulatory requirements.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>38</td>
<td>Performs Capacity Planning</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>39</td>
<td>Manages Internet Protocol (IP) Addresses</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>40</td>
<td>Designs, Develops and/or Reviews Radio Technical Integration and Interface Specifications</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>41</td>
<td>Conducts Radio Field Coverage Surveys</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>42</td>
<td>Performs Radio Network, System, and Radio Frequency (RF) Engineering</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>43</td>
<td>Reviews and Comments on Construction Plans</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>44</td>
<td>Adds Radios to a Radio Network</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>45</td>
<td>Implements Radio Programming to Field Radios</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>46</td>
<td>Develops Security Policy and Procedures within Public Safety Radio System Environments</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>47</td>
<td>Manages Access Control to Secure physical space</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Line #</td>
<td>Codes: &quot;R&quot; - Required  &quot;P&quot;- Preferred  &quot;X&quot; - Relevant Experience(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>Implements Technical, Computer, and Radio Systems Access Controls</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>Manages Shared Federal and MWAA Encryption Keys</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>49a</td>
<td>Programs Encryption into Radio Subscribers</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>Implements Automated Virus Control and Protection System</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Reserved</td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>Provides Radio User Assistance</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>Conducts User Satisfaction Surveys</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>Develops Training Programs and Materials</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>54a</td>
<td>Conducts Training 1. Provides guidance and training to less experienced analysts. 2. Advises staff on new industry of product issues, technical problems, priorities, and methods.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>Performs Daily Radio Facility Site and System Checks</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>Provides Radio User Field Support Services</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>Provides First Response to User Requests and Problems</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>Performs Analysis, Troubleshooting, Solution Delivery of Radio Networks</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>Conducts Radio Preventative Maintenance Services</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>Installs radio systems in vehicles and office space</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>Implements 800 MHz Radio Templates</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>Programs and Configures 800MHz Radios</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>Installs/Integrates and maintains multi-position Intercom Systems in Fire Apparatus and other specialized vehicles.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>Installs, Replaces, and Repairs Roof Mounted Antennas -</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>Installs, Replaces, Repairs 800 MHz 'In-Building' Radiating Antenna Systems</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>66</td>
<td>Administers Contracts</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>Prepares Solicitation Documents</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>Validates Contract Performance</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>Reviews Quality of Work Performed</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>Performs Radio System Network Maintenance</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>Plans, Performs and/or Supports Radio PM Service</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>Conducts 1st Tier Maintenance on Radio Systems</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
## Labor Categories and Descriptions

<table>
<thead>
<tr>
<th>Line #</th>
<th>Codes: &quot;R&quot; - Required &quot;P&quot; - Preferred &quot;X&quot; - Relevant Experience(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>73</td>
<td>Conducts 2nd Tier Radio Maintenance on Radio Systems</td>
</tr>
<tr>
<td></td>
<td>X X X X X X X X X X</td>
</tr>
<tr>
<td>74</td>
<td>Conducts 3rd Tier Radio Maintenance on Radio System</td>
</tr>
<tr>
<td></td>
<td>X X X X X X X X X</td>
</tr>
<tr>
<td>75</td>
<td>Maintains Radio System And Subscriber Repair Records</td>
</tr>
<tr>
<td></td>
<td>X X X X X X X X X</td>
</tr>
<tr>
<td>76</td>
<td>Uses Test Equipment to Diagnose Radio or Network Problems</td>
</tr>
<tr>
<td></td>
<td>X X X X X X X X X</td>
</tr>
<tr>
<td>77</td>
<td>Performs 800 MHz Battery Maintenance and Replacement</td>
</tr>
<tr>
<td></td>
<td>X X X X X X X X X</td>
</tr>
<tr>
<td></td>
<td>• Uninterrupted Power Supplies</td>
</tr>
<tr>
<td></td>
<td>• Battery Maintenance</td>
</tr>
<tr>
<td></td>
<td>• Battery Conditioning</td>
</tr>
<tr>
<td>78</td>
<td>Administrative Services</td>
</tr>
<tr>
<td>79</td>
<td>Performs Budget Administration</td>
</tr>
<tr>
<td></td>
<td>• Develops Budget Estimates</td>
</tr>
<tr>
<td></td>
<td>• Controls/Manages Budget Execution</td>
</tr>
<tr>
<td></td>
<td>• Quarterly Reviews</td>
</tr>
<tr>
<td></td>
<td>• Budget Reporting</td>
</tr>
<tr>
<td></td>
<td>X X X X X X X X X X</td>
</tr>
<tr>
<td>80</td>
<td>Performs Procurement Management</td>
</tr>
<tr>
<td></td>
<td>• Prepares Purchase Requests</td>
</tr>
<tr>
<td></td>
<td>• Prepares Statements of Work</td>
</tr>
<tr>
<td></td>
<td>• Proposal Evaluations</td>
</tr>
<tr>
<td></td>
<td>• Invoice Reconciliation and Approvals</td>
</tr>
<tr>
<td></td>
<td>X X X X X X X X X X</td>
</tr>
<tr>
<td>81</td>
<td>Performs Materials Management</td>
</tr>
<tr>
<td></td>
<td>• Request Assets, Spare Parts, and Supplies</td>
</tr>
<tr>
<td></td>
<td>• Receive and Control Assets</td>
</tr>
<tr>
<td></td>
<td>• Store Spare Parts and Supplies</td>
</tr>
<tr>
<td></td>
<td>• Maintain Inventory Records</td>
</tr>
<tr>
<td></td>
<td>• Receive - Issue</td>
</tr>
<tr>
<td></td>
<td>X X X X X X X X X X</td>
</tr>
<tr>
<td>82</td>
<td>Provides Escort in SIDA and secure facilities</td>
</tr>
<tr>
<td></td>
<td>X X X X X X X X X X</td>
</tr>
<tr>
<td>83</td>
<td>Reporting/Studies</td>
</tr>
<tr>
<td></td>
<td>1. Conducts Feasibility Studies</td>
</tr>
<tr>
<td></td>
<td>X X X X X X X X X X</td>
</tr>
<tr>
<td></td>
<td>2. Contributes to studies by providing costing models, reports, and technical solutions.</td>
</tr>
<tr>
<td>84</td>
<td>Space Management</td>
</tr>
<tr>
<td></td>
<td>X X X X X X X X X X</td>
</tr>
<tr>
<td>85</td>
<td>Personnel Actions, Time Reporting</td>
</tr>
<tr>
<td></td>
<td>X X X X X X X X X X</td>
</tr>
</tbody>
</table>

*Page C-5 to C-7*
<table>
<thead>
<tr>
<th>Line #</th>
<th>Codes: &quot;R&quot; - Required  &quot;P&quot; - Preferred  &quot;X&quot; - Relevant Experience(s)</th>
<th>Senior Project Manager  Coordinator</th>
<th>Radio and Wireless Technical Services</th>
<th>Communications Analyst  Engineer</th>
<th>Supplemental Radiating System Field Engineer</th>
<th>Radio Frequency Engineering Planner</th>
<th>Senior Radio (Infrastructure) and Networking Technician</th>
<th>Communications Integration Technician</th>
<th>Radio Maintenance Technician</th>
</tr>
</thead>
<tbody>
<tr>
<td>86</td>
<td>Provides Project and Planning Management</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>87</td>
<td>Develops Department Five Year Plan</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>88</td>
<td>Identifies Strategic Initiatives</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>89</td>
<td>Applies Safety</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>90</td>
<td>Radio Tower and Roof top Operations</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>91</td>
<td>Climbs RADIO towers</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>92</td>
<td>Performs tower corrective and preventative maintenance</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>93</td>
<td>Calculates and Verifies point-to-point signal path levels</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>94</td>
<td>Creates detailed documentation of work performed on tower/rooftop facilities</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>95</td>
<td>Inspects and maintain antenna transmission line, radio tower lighting system, and related equipment</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>96</td>
<td>Inspects communication towers to assess and/or schedule preventative or remedial maintenance</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>97</td>
<td>Installs connector ground kits</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>98</td>
<td>Installs/removes radio system components, cables and antennas</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>99</td>
<td>Interprets blueprints, diagrams, and schematics</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>100</td>
<td>Makes preliminary line-of-site surveys from communication towers</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>101</td>
<td>Operates electronic diagnostic equipment (e.g. comm service analyzers, digital voltmeters, Spectrum Analyzers, Time Domain Reflectometers [OTDR/TDR's], Wattmeters, etc.).</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>102</td>
<td>Plans and schedules tower inspections, repairs and maintenance</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>103</td>
<td>Uses OSHA Approved climbing and safety gear</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>104</td>
<td>Radio System Engineering</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>105</td>
<td>Analyzes Radio Problems and Needs (Interference, Intelligibility, Clarity, Etc.)</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>106</td>
<td>Attends Meetings, Conferences, and Events, as Directed by the COTR</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>107</td>
<td>Conducts Engineering Studies</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
<td>X X X X X X X X X X X X</td>
</tr>
<tr>
<td>Line #</td>
<td>Codes: &quot;R&quot; - Required  &quot;P&quot; - Preferred  &quot;X&quot; - Relevant Experience(s)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>Designs Radio Communications Sites</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>109</td>
<td>Evaluates, and Implements (multiple vendor) Interconnect Equipment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>Develops Bid Specifications and Requests for Proposal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>111</td>
<td>Develops Engineering Project Proposals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>112</td>
<td>Develops Technical Solutions to Radio Problems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>113</td>
<td>Evaluates New Radio System Products and Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>114</td>
<td>Evaluates Radio System Electrical Power Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>115</td>
<td>Evaluates Vendor Responses to Proposals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>116</td>
<td>Inspects Radio System Technical Work for Compliance with Standards and Specifications.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>117</td>
<td>Performs Projects Assigned by COTR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>118</td>
<td>Plans, Designs, Engineers, Configures and Implements Radio Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>119</td>
<td>Prepares Communications System Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>120</td>
<td>Prepares Detailed Construction Plans</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>121</td>
<td>Prepares Operational Procedures for Communication Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>122</td>
<td>Develops and Maintains the Authority’s Radio-Communications Continuity of Operation Plan (R-COOP) and Radio Communications Intra- and Inter-Operational Plan (CIIOP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123</td>
<td>Prepares Preliminary and Long-Range Plans, Estimates, and Budgets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123a</td>
<td>Prepares Radio Propagation Exhibits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>124</td>
<td>Prepares/Write Technical Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>125</td>
<td>Provides Technical Advice in the Selection, Procurement, Installation, Testing, and Acceptance of Radio Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>126</td>
<td>Researches Emerging Radio System Technologies, Services and Equipment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>127</td>
<td>Reviews and Comments_ Detailed Construction Plans</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>Verifies Proper Frequency Use and Assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX E

CONTRACT POSITION DESCRIPTIONS
Position Title: Senior Project Manager

Primary Duty Station: Ronald Reagan International Airport (DCA)/Dulles International Airport (IAD)

Availability/Utilization: Normal Business Hours

Nature of Work: Manages ‘Day-to-Day’ projects and develops Department strategic and project plans, solicitation packages (statements of work, evaluation criteria, schedules, vendor instructions) to support acquisition of public safety and Authority-wide wireless and radio system requirements, on behalf of the Department Manager.

Responsibilities: Staffs the Department’s Project Management position, as identified and justified in the Wireless and Radio Systems Network Management Plan. Provides project management services. Develops Department budgets for operations and maintenance and COMIP. Prepares quarterly financial reviews, analyses and assessments. Develops solicitation packages in support of Department acquisitions. Develops Departmental standards, operational protocols, and procedures. Supports Department strategic planning. Consults with department managers, provides planning, system analysis, and project management support. Prepares technical documentation.


Abilities: Able to develop standards and procedures based on best practices and lessons learned in support of the Department and Authority. Supports Department in short and long term strategic planning efforts. Can apply detailed analysis to analyze, develop and justify department level budgets. Applies organizational and situational awareness to coordinate with other departments in developing goals and strategies in support of Departmental mission. Monitors budget execution and advises the Department Manager of issues requiring management action. In coordination with MA-20, administers the Asset Capitalization program for the Department.

Required Education and Experience: (25 Years of documented experience)
Strategic and Operational Planning. Forecasting and budgeting of capital and operational expense budgets. Project initiation, planning, execution, monitoring and control and closeout.

Bachelors or master's degree in business or public administration

Required Certifications or Licensure:

Proficiency or Skills Testing Required:
Metropolitan Washington Airports Authority
MA-630 Wireless and Radio
Contract Position Description

**Position Title:** Radio and Wireless Technical Services Coordinator

**Primary Duty Station:** Ronald Reagan International Airport (DCA Hangar 5A)

**Availability/Utilization**
Normal Business Hours

**Nature of Work:** Independently provides administrative and technical operational support to the dynamic, day-to-day, business of the Radio and Wireless Systems Department, in accordance with established procedures. Independently monitors the 800 MHz radio system and hardware/software alarms at the Network Operations Center (NOC) and reports alarm conditions to the Department Manager and appropriate field technical supervisors/personnel. Supplies Tier I/II support and coordinates Tier III and Tier IV services.

**Responsibilities:** Plans, Performs and Manages Radio Preventative Maintenance services for 3000 radios. Interfaces between the department and ‘end-users’. Manages $24M Radio System assets to track high-value assets moved between the airports, to/from external servicers, returned to users, reassigned and within the airport environment. Maintains automated inventory and $23M infrastructure and assets. Tracks work order aging to determine vendor compliance with repair-return contract terms. Maintains, updates and Performs quality review of the Department’s automated Work Order Entry input and installation services. Serves as the Department time manager, recording staff and contractor work hours, on behalf of the Department Manager. Assists with the administration of support contracts for radio services and wireless projects, under the guidance of the Department Manager. Assists with department budget preparation and computer-based cost accounting, P-Card reconciliation and Parking management. Supports FCC compliance activities.

**Knowledge:** Computer Literacy. Principles and practices of organization, planning, records management, accounting, and general office administration. Ability to operate Radio Management terminal equipment. Setup and Use of communications service analyzer. The ability to read/write programming files to a subscriber radio, determine firmware and “flash” equipment to new firmware level.

**Skills:** Database Entry and Keyboarding. Word Processing. Handling of business telephone calls utilizing key telephone and voice mail systems. Use of portable and mobile radios. Filing, Copying and operation of general office equipment (Facsimile, document scanners, copying machines). Writing, Accounting, analytical, and problem solving skills.

**Abilities:** Maintains automated databases and spreadsheets, in support of the department budget, radio inventory and critical infrastructure spare parts, with minimal guidance. Disseminates information to department staff and department constituencies. Prepares correspondence, maintains program files and orders department equipment and supplies. Schedules and coordinates conference calls and face to face meetings with staff, mutual aid and county, state and federal agency stakeholders. Coordinates and tracks the status and receipt of progress reports from supporting contractors and staff. Tracks internal communications, including projects and task deadlines, requests from Authority offices and local jurisdictions and stakeholders. Reads and understands construction documents and creates computer-based drawings, plans, diagrams and layouts based on notes, sketches, calculations, specification sheets and other data. Ability to follow verbal or written instruction.

**Required Education and Experience:** (5 Years of documented experience)
Microsoft Office Products (MS-Word, MS-Excel, MS-Access, MS-Power Point, MS-Outlook, MS-Visio). Ceridian and DelTek Time-keeping Systems. Motorola MOSCAD Alarm and Motorola Private Radio Network Management suite (NMS) Motorola Centracom Gold Elite Alias Database Manager (ADM) and GENZAI diagnostics
High School Graduate or GED. Knowledge of mobile installation best practices.

**Required Certifications or Licensure:**

**Proficiency or Skills Testing Required:** Excel, Motorola CPS, ability to determine and flash subscriber firmware. Operation of MOSCAD Alarm and Motorola Private Radio Network Management suite (NMS), Motorola Centracom Gold Elite Alias Database Manager (ADM) and GENZAI diagnostics application.
Position Title: Senior Radio Engineer
Primary Duty Station: Ronald Reagan International Airport (DCA Hangar 5A)
Availability/Utilization Normal Business Hours and Emergency/ 24 x 7 availability

Nature of Work: Technical lead for maintenance, capacity or coverage improvements involving land mobile radio systems. Provides Tier I, II, III and coordinates Tier IV technical support. Operates with minimal supervision or oversight to evaluate systems, ensure compliance, and propose enhancements to equipment.

Responsibilities: Assists the manager with day-to-day operations and technical support involving mission-critical public safety and public service airport radio systems

Conducts engineering, research and analysis to develop and design ‘in house’, ‘cost-effective’ solutions that address complex technical challenges within a unique and challenging environment.

- Provides and Supports system planning, design, development, installation, optimization and commissioning
- Provides Project, Planning Management and Quality Review
- Performs Radio Network Administration and Technical Administration
- Monitors Systems Alarms and Alerts 24 x 7
- Monitors and Analyzes Performance Metrics
- Performs Frequency Management, Coverage and Capacity Planning, Evaluation and Implements solutions
- Optimizes, Adjusts and Balances Radio Network /Conducts FCC Compliance activities
- Conducts. Coordinates and/or Assists Radio Maintenance, as required
- Maintains Radio Systems, System Components, Radio Configurations and Accurate Records
- Develops templates and provides field radio Programming
- Performs Field Interference Analysis
- Operates sophisticated test equipment to examine/analyze radio systems
- Prepares Technical Reports
- Interprets blueprints, diagrams and schematics
- Reviews technical plans and comments.
- Prepares Solicitation Documentation, Administers Contracts, Validates Contract Performance.
- Assists in developing purchase requests and procurement justification.
- Provides Training to Authority and contractor staff on the operation and maintenance of test and system equipment in support of personnel cross function
- Performs projects assigned by the COTR

Skills:

Abilities:
Establish and maintain working relationships with equipment vendors and service providers for the supply, installation, optimization and maintenance of Authority-owned and managed radio systems. Conduct research and analyze results to develop and design in-house solutions for complex technical problems. Coordination and facilitation of field meetings and site walks for equipment installations. Verification of deployed technologies for conformance with acceptable standards of operation. Monitor and review radio system performance metrics. Leads FCC regulatory compliance activities. Conducts radio system planning, design, development, installation, optimization and commissioning. Provisioning and introduction of new subscriber equipment to networks. Documentation of moves, adds, changes to radio system infrastructure equipment. Emergency response to repair and restore communications systems during major failures.

Required Education and Experience
Installation, maintenance, and operation of complex trunked radio communications systems and networks.

20 Years of documented experience, technical training. Experience in Frequency Coordination (required) Experience in Public Safety communications and/or operations (preferred)

Required Certifications or Licensure: FCC General Radio Operators License or equivalent


Note: Position subject to recall and holdover during weather and other emergencies
Position Title: Communications Analyst
Primary Duty Station: Ronald Reagan International Airport (DCA Hangar 5A)
Availability/Utilization: Normal Business or Adjusted Schedule

Nature of Work: Provides day-to-day project management for large communications system projects, such as the 800 MHz Rebanding Program. Operates under broad general guidelines with minimal daily supervision to achieve project goals. Provides regular updates on project progress and expenditures.

Responsibilities: Responsible for administrative and cost-management of MWAA's 800 MHz Rebanding Program, on behalf of the Department Manager.


Abilities: Able to develop and justify project plans, budgets, schedules and progress reports. Coordinates with departments, contractors, and mutual aid partners to complete scheduled work on established project milestones. Can maintain automated databases and spreadsheets to track project progress, status, and budgets. Tracks radio inventory and deliveries. Disseminates project related information to team members. Maintains project files. Schedules and coordinates conference calls and face to face project meetings.

Required Education and Experience: (10 Years of documented experience)
Technical and/or Financial project management and Administration.

Required Certifications or Licensure: Proficiency or Skills Testing Required:
Position Title: Senior Network Engineer
Primary Duty Station: Ronald Reagan International Airport (DCA Hangar 5A)
Availability/Utilization: Normal Business Hours and Emergency/24 x 7 Availability

Nature of Work: Develops, Implements (installation, configuration), Operates, and Maintains the Radio -Network Local Area Network infrastructure and interfaces supporting the Authority’s Wireless and Radio systems on a 24 x 7 basis. Works independently or with other Authority personnel or contractors with minimal supervision or oversight. Provides routine status and progress reports to MA630 to communicate network availability and security. Reports network malfunctions and corrective actions taken to the Manager MA-630 in a timely manner, using a format acceptable to the Authority.

Responsibilities: Works with Department staff to install network infrastructure and resolve problems. Supports development of security policy and procedures manual. Enforces Authority Information Security Standards (ISS) to protect the Radio LAN (R-LAN). Implements and manages network policies, procedures and standards. Provides Tier I/II/III/IV support for network equipment. Maintains configuration standards and management database to provide accurate, complete, timely, formal documentation of authorized network reconfigurations. Establishes and maintains a configuration baseline that conforms to the actual internetworking environment, as approved by the Manager MA-630. Maintains IP-schema. Provides network engineering for Department projects. Assists in the development and execution of contingency plans for network software and hardware failures. Devises solutions to operational problems with installed equipment. Provisions, configures, restarts and/or refreshes network components.


Required Education and Experience: (5 Years of documented experience)
Network Engineering and Administration
Associate's or bachelor's degree in electrical engineering or engineering technology with an emphasis on telecommunications or networking (preferred)

Required Certifications or Licensure:
Cisco Certified Network Professional (CCNP)

Proficiency or Skills Testing Required: Wiring and Interconnection methods. Basic hand tools. Basic and moderately complex electronic or signal quality measurements. Fiber Optic technologies. TCP/IP addressing. Network troubleshooting. TIA Network cable terminations (TIA568) and tests. CISCO Networking, Excel
Position Title: Supplemental Radiating System (SRS) Field Engineer
Primary Duty Station: Ronald Reagan International Airport (DCA Hangar 5A)
Availability/Utilization: Normal Business Hours and Emergency / 24 x 7 Availability

Nature of Work: Performs engineering to Design, Engineer, Configure, Install, Integrate, Optimize, Test and Maintain the Authority’s complex, distributed Supplemental Radiating System. Tier I, II, III, IV Support. Makes incremental or major changes to the system design. Project manages and performs technology upgrades and functionality. Operates with minimal direction and general guidance, providing status and operational reports, as needed to the manager.

Responsibilities: Operationally monitors, provides preventive maintenance, repair, and enhancement or expansion of the SRS at all MWAA locations. Liaisons with vendors, contractors on projects related or impacting to SRS operation. Coordinates and works with Staff, contractors, internal customers and wireless carriers in a professional manner to ensure optimal coverage and access to MWAA communications systems. Updates ‘As-Built’ documentation for further use by the Authority or contractors. Maintain non-SRS radio communications and antenna systems. Plans major and minor SRS-related projects including the preparation of schedules, budget estimates, material lists and reports for MA-630 management review.

Knowledge: Detailed understanding of bi-directional amplifiers, fiber-fed and coaxial-based distributed antenna systems and MWAA supplemental radiating systems through existing ‘as-built’ documentation and hands-on experience with this system or primary system engineering on a system of demonstrated comparable complexity. Multi-mode and single mode fiber optic technologies. Radio frequency engineering and signal analysis. Electrical engineering formulas and mathematical calculation or manipulation of information. IP-based Communications status network reporting/SCADA/alarm systems. RF passive and active components and usage (antennas, splitters, filters, isolators, directional couplers, cabling, connectors and connectorization).

Skills: Setup and operation of complex test equipment (spectrum analyzers, time domain reflectometers, communications system analyzers, network cabling analyzers) to evaluate installed equipment and ambient RF environment. Installation, testing and documentation of RF coaxial cabling, fiber-optic cabling and CAT5 LAN/Internet cabling. Preparation, connectorization, splicing, termination, and verification of network, RF coaxial and fiber optic cabling. Preparation of equipment lists, bills of material, cost estimates, statements of work and purchase requests. Minor repair, installation, or replacement of various cables and equipment. Modification, adjustment, alignment, or optimization of repaired or replaced equipment to conform with signal levels or engineering drawings. Autocad drawing development and maintenance. Basic Project Management (initiation, planning, execution, monitoring and control, and closeout). Microsoft Office Products (MS-Word, MS-Excel, MS-Access, MS-Outlook)

Abilities: Modify drawings and documentation using AutoCAD or similar software applications. Prepare engineering designs and perform calculations to support the modification of the current SRS for expanded coverage area and additional spectrum. Monitor existing systems and troubleshoot problems or evaluate performance and system degradation. Continuously monitor the Authority's SRS status and 800 MHz trunked radio noise floor at both Dulles and National. Work with and provide guidance or direction to the Authority’s SRS maintenance contractor. Perform on-site installation tasks in support of the SRS. Perform minor installations and repairs of cable for all Authority RF, networking, and fiber cables as required. Install SRS equipment for minor or major upgrades or inspect the work of subcontractors performing this task. Correctly test, align and optimize the SRS after repair of modifications. Supervise projects to maintain schedule, budget and performance. Identify and Review delivered materials against packing slips. Evaluate substitute or replacement equipment/assemblies.

Required Education and Experience: (10 Years of documented experience)
Distributed antenna systems engineering, installation, and maintenance on a system of comparable size and complexity. Fiber Optic Experience; Manufacturer Technical Training by Allen Telecom, Kaval, Powerwave, Andrew, AFL, AXELL, TX-RX, and Anritsu. Electronics training or associate's degree in electrical engineering technology with emphasis in telecommunications.

Required Certifications or Licensure: BiSCI certification preferred.


Note: Position subject to recall and holdover during weather and other emergencies.
Position Title: Radio Frequency Engineering Planner
Primary Duty Station: Ronald Reagan International Airport (DCA Hangar 5A)
Availability/Utilization: Normal Business or Adjusted Schedule

Nature of Work: Represents the Authority in strategic Regional Council of Government public safety technical Planning, Governance and Policy committees. Conducts cost/benefit analysis and liaisons with Authority stakeholders to determine project impact. Provides regular written reports on activities and status and seeks Authority approval. Project staffs to implement approved plans. Provides SME technical document review and comment systems to technical reports (including the ‘Next Generation Radio System Study’, Rebanding processes, CWAS management, spectrum modifications and Tenant wireless construction requests. Additional responsibilities include:

- Attending FCC and Region 20 Technical meetings to provide 700 MHz system build status, D-Block license status and Public Safety Wireless Issues/Solutions.
- Project management of the multi-phased NCRnet Technical project implementation
- Provides daily oversight and Inspection of Rebanding contractor and Deliverables
- Reviews FCC Notices of Proposed Rule Making (NPRM) to determine impact on the Authority
- Coordinates with Counsel to Develops management response for consideration.
- Determines FCC Ruling impacts.
- Conducts FCC Compliance Activities
- Identifies Federal Funding initiatives and opportunities
- Serves as technical/project liaison to the NCR State Administrative Agent (SAA) for (federal) grants
- Supports Rebanding Activities through attendance at NCR Regional Rebanding
- Prepares Technical Documentation
- Plans, Performs and/or Supports Quality Review of Radio Preventative Maintenance Services
- Reviews and Conducts Engineering Studies and Evaluates Bid Specs
- Performs Evaluations of contracted services
- Participates in technical support contract document review
- Validates Contract Performance
- Monitors Performance Metrics
- Interpret blueprints, diagrams and schematics
- Prepares Technical Reports, Cost Estimates and Budgets
- Contributes to Reporting Studies and Cost Models
- Provides Technical Administration
- Performs Budget Administration

Responsibilities: Schedules service contract projects that include ALL annual preventive maintenance processes on portable and mobile radios and wireless infrastructure equipment. Reviews, comments and participates in contract development supporting maintenance contracts. Performs financial cost benefit analyses on new wireless initiatives for the Authority. Performs as Subject-Matter-Expert on FCC processes and procedures involving use of public safety wireless spectrum.

Knowledge: Comprehensive understanding of FAA radio communications procedures for ground and air crews. Public safety communications technologies and regulations. FCC 800 MHz rebanding processes. Federal funding mechanisms and processes (PSIC/UASI).

Abilities: Provides Quality Control and Assurance by developing uniform standards, protocols, and procedures for the Radio Support team. Prepares and submits grant applications within timelines. Administers and Ensures compliance with awarded grants requirements. Represents the interests of the Authority on interoperable communications issues in the National Capital Region, the Metropolitan Washington Council of Governments and regional standards boards. Prepares written comments on FCC regulatory and enforcement actions, and track activities. Develops strategies to meet both current and future FCC mandates on current Public Safety radio spectrum. Researches, reviews and recommends new and updated wireless technologies to address FCC mandates and to improve communications.

Required Education and Experience: (10 Years of documented experience)

Technical engineering and strategic business planning of advanced telecommunications systems.
Bachelor’s or Master’s in Electrical Engineering (Required)
BSEE and Master’s in Business Administration (Preferred)

Required Certifications or Licensure:
BSEE

Proficiency or Skills Testing Required:
Position Title: System Analyst
Primary Duty Station: Ronald Reagan International Airport (DCA Hangar 5A)
Availability/Utilization: Normal Business Hours and Emergency/24 x 7

Nature of Work: Single technical/operational Department point-of-contact for the Authority’s Public Safety Communications Center (PSCC) 24 x 7. Provides daily operational and technical support to the PSCC. Develops and coordinates mutual aid/interoperability with all Local, State and Federal partners. Develops, Plans, Conducts and/or Evaluates yearly DHS-compliant communications exercises involving stakeholders and internal/external partners. Works with representatives of other departments and outside agencies at various management and support levels and with minimal direction to develop and execute inter-operational communications tactical plans. Provides frequent reports and status updates to Department Manager. Develops and maintains internal and external radio guidelines, procedures and standards. Administers the Department’s Asset, Work Order and ID Management automated system. Serves on Regional public safety Committees as a subject-matter-expert in Encryption and Interoperation. Manages shared Federal, Regional and Authority-wide encryption keys and equipment as the Authority’s Radio Department ‘Crypto Officer’. Develops and provides all training for Authority radio users. Maps department and PSCC functional processes involving radio into flow chart format for analysis, discussion and/or process modification to meet goals.

Responsibilities: Project and Planning management. Provides technical and administrative support as project lead for the Department’s Asset, Work Order and ID Management automated system. Serves as point of contact and provides technical support to the Public Safety Communications Center. Serves as Lead Communications Unit Leader (COM-L) for the Authority and operates/maintains the Authority’s Communications Support Unit (CSU). Provides certified COM-L, COM-T and NIMS training. Serves as a member of the National Capital Region (NCR) Incident Management Team. Develops and Maintains the Authority’s Radio Communications Continuity of Operations and Radio Communications Intra- and Interoperability Operations Plans (R-COOP and R-CIIOP, respectively.) Attends meetings, conferences and events.


Abilities: Radio template development and subscriber equipment programming. Training/Education and Experience in Public Safety radio communications plans, practices and procedures. Supports emergency events with Authority-owned assets and deploys equipment to establish communications pathways. Responds to planned or unscheduled events for Authority.

Programs and Configures and Maintains interoperable communications gateways.
**Required Education and Experience:**
(10 Years of documented experience)
High school graduate with electronics training, or associate's degree in electrical engineering technology and/or Emergency Management
Public Safety technical communications and/or operations experience
Management of emergency communications and resource planning
Incident command structure and principles
Land Mobile Radio encryption management practices
Land Mobile Radio Spectrum Management
Trunked and Conventional Subscriber Radio programming
Interoperation resources / Ability to program gateways
Manufacturer training (MSV, CODAN, JPS/Raytheon)

**Required Certifications or Licensure:**
High school graduate with electronics training, or associate's degree in electrical engineering technology and/or Emergency Management
FCC General Radio Operators License or equivalent
FEMA Homeland Security Exercise and Evaluation (HSEEP) Program
FEMA HSEEP Trainer (preferred)
National Incident Management System (NIMS) Trainer certification (preferred)
Department of Homeland Security Communications Leader (COM-L) certification
Department of Homeland Security Communications Leader Trainer certification (preferred)
Encryption Management principles and practices
Land Mobile Radio Spectrum Management
Manufacturer training (MSV, CODAN, JPS/Raytheon)

**Proficiency or Skills Testing Required:**

Note: Position subject to recall and holdover during weather and other emergencies
Position Title: Senior Radio and Networking Technologist
Primary Duty Station: Ronald Reagan International Airport (DCA)/Dulles International Airport (IAD)
Availability/Utilization: Normal Business Hours and Emergency 24x7

Nature of Work: The Department operates a unique network extension between the airports. The Radio-LAN (R-LAN) is not an Enterprise or “user focused” network. The R-LAN has no Active Directory or Domain but operates as a “lights-out” data center where users interact minimally with the systems and devices that constitute the network. This radio system ‘extension’ distributes radio system metrics, system updates and alarm notifications. It supports data protection management, IP surveillance and operates under local Group Policies implemented to support efficiency, stability, and survivability in the presence of attacks, failures, or accidents. WINS architecture supports the diversity of operating systems deployed across the network: (Windows 2000, Windows 2000 Server, Windows 2000 Advanced Server, Windows XP, Windows XP SP1-SP3, Windows Server 2003 Standard, Windows Server 2003 Enterprise SP2, Windows Server 2003 R2, Windows Server 2003 R2 SP2, Windows Server 2003 Datacenter SP2, Windows Server 2008 Standard, Windows Server 2008 R2 SP2, Linux and Windows 7). The diversity of operating systems is the result of licensing, supported legacy systems and/or lack of vendor product compatibility. Systems supported by this position are provided in Appendix C.

The Senior Radio Networking Technologist supports systems and applications operating across the Radio-LAN. Services provided include Tier I/II/III/IV and include, but are not limited to:

- Daily Interface with the Senior Network Engineer addressing the unique technical administration/configuration of the Radio LAN/WAN required to support the users and systems 24x7
- Designing/Implementing/Configuring/Operating/Managing and Supporting all servers, workstations and automated data backup systems supporting the radio systems (See Appendix C)
- Performing or supervising the work of other contractors in the support of advanced technologies
- Maintaining security/access at radio tower sites and rooms and supporting/managing all elements of the ‘real-time’ critical infrastructure alarm notification system.
- Serving as the Department’s Computer Information Security Officer (CISO) to oversee department compliance with the Authority’s Information Systems Security Standard (ISS) and other security requirements
- Maintaining availability/monitoring critical alarms and alerts 24x7
- Integrating site security, metrics, intrusion and environmental status detection systems
- Maintaining the IAD and DCA Radio Network Operations Center Systems
- Performing network performance analysis of the LAN
- Performing analysis, troubleshooting and solution delivery of radio networks, in accordance with best industry Operations and Security practices and the Authority ISS.
- Performing and Documenting radio network, system and RF engineering services
- Debugging, Testing and Documenting software problems encountered and developing/testing and documenting corrective solutions.
- Designing, developing and reviewing radio technical integration and interface specifications
- Performing radio system network maintenance
- Providing project and planning management
- Designing radio communications sites
- Preparing communication system specifications
- Preparing technical reports
- Providing recommendations and implementing approved plans for networking and security systems.
Senior Radio and Networking Technologist

Responsibilities: Act as Radio Systems Network Support Administrator for MA630. Researches, designs, implements, maintains and troubleshoots information systems and technology solutions. Installs, implements, and repairs CCTV and IP-Based Security Cameras. Provides users with network technical support, responding to their needs and questions regarding access to resources on the network, including the Radio- Local Area Network (RLAN). Supports administration of Motorola trunked infrastructure. Establishes and documents standards and procedures, in accordance with security requirements. Monitors Alarms/Alerts 24x7 basis and maintains availability as a critical service provider.


Abilities: Designs, implements and repairs computer systems. Troubleshoots and repairs complex electronic systems and devices. Installs, configures, upgrades, troubleshoots and repairs network hardware and software components, including 802.11 Wireless Security Systems. Troubleshoots networks to isolate and diagnose common problems. Installs, upgrades, and Configures network printing, directory structures, rights, security, and software. Establishes network user accounts, user environment, directories, and security for networks. Monitors network and performs necessary maintenance or administration to support and ensure network availability for all authorized system users. Supervises other contracted network support and client server specialists. Can plan, coordinate, and implement network security measures. Modifies, debugs, tests, and documents software for operating systems. Installs IP-based and fixed intrusion detection, surveillance, access control, and smoke/fire detection system devices. Identifies and prepares physical pathways and support systems for new cabling systems installations. Plans, pulls, terminates, tests, and documents structured cabling systems. Performs approved alterations and additions to systems.

Required Education and Experience: (10 Years of documented experience)

High school graduate with electronics training or associate's degree in electrical engineering technology with emphasis in computers and networking.

Required Certifications or Licensure: MSCE certification. EET or equal. EDT (preferred), FCC General Radio Operator's License. Certified Fiber Optic Technician/Installer or experience (preferred). Microsoft Operating System certifications.


Note: This position is subject to recall and holdover during weather and other emergencies.
Position Title: Field Radio Support Tech./Radio Communications Integration Tech.
Primary Duty Station: Ronald Reagan International Airport (DCA Hangar 5A)
Availability/Utilization: Normal Business Hours and Emergency

Nature of Work: Supplies high-volume and consistent-quality integration of communications, special systems and emergency lighting into Public Safety and Public Service vehicles. Challenging and unique installations require design/fabrication of brackets/mounts, modification of vehicular electrical systems and the use of ‘best installation’ practices. Position also provides field radio system technical support and programming services. Tasks include but are not limited to:

- Physical and electrical integration of multiple radios, systems and controls into a wide variety of motor vehicles and boats
- Installation, Removal, Transfer of public safety emergency equipment between vehicles
- Design /Document installation standards and Implementing a production plan
- Installing/Maintain and Repair emergency vehicle warning systems and associated wiring
- Integrating fire apparatus, headset/intercoms, land mobile and aviation radios, mobile video, radar, emergency lighting, switch panels, license plate readers and mobile computer terminals
- Providing Tier I,II,III, IV field support and preventative maintenance,
- Providing field radio programming, encryption loading and firmware updates
- Maintaining accurate radio system and equipment asset records
- Preparing and maintaining technical ‘As-Built’ system documentation
- Conducting FCC compliance activities
- Conducting user training
- Performing daily radio facility site and system checks
- Operating sophisticated test equipment to diagnose antenna and communication systems
- Assists Developing project plans
- Interpreting blueprints, diagrams and schematics
- Attending meetings, conferences and events, as requested by the COTR
- Performing projects assigned by the COTR

Responsibilities:
Installs new hardware, remove old hardware and maintain existing hardware. Program radios and Provide firmware updates to radio subscribers. Participate in maintenance of site radio and storage rooms, radio system spare equipment stock levels, and radio user records. Develop and maintain accurate records of computer systems, electronic communications system and equipment performance, work accomplished and other information, as appropriate.


**Field Radio Support Tech /Radio Communications Integration Tech (Page 2)**

**Abilities:** Information gathering and assimilation from customer complaints or problem reports. Provides field coordination, escort services and guidance to multiple contractors working on radio/wireless projects. Schedules, coordinates, facilitates or performs preventive maintenance to ensure compliance with manufacturer requirements. Maintains accurate work reports and records of test results.

**Required Education and Experience:** (5 Years of documented experience) Installation, maintenance and repair of electronic and radio communications systems, focusing on vehicular electronics. High school graduate with electronics training and/or associate’s degree in electrical engineering technology.

**Required Certifications or Licensure:** MECT or EVT, CET, NABER, GROL or industry equal.


Note: This position is subject to recall and holdover during weather and other emergencies.
Position Title: Radio Maintenance Technician
Primary Duty Station: Ronald Reagan National Airport (DCA)/Washington Dulles International Airport (IAD)
Availability/Utilization: Normal Business Hours and Emergency

Nature of Work: Provides radio communications system maintenance and field technical services. May perform and/or supervise installation and maintenance of radio communications subscriber equipment.

Support includes but is not limited to:

- Conducting Tier I, II, III, IV radio subscriber troubleshooting and solution delivery
- Coordinating and participating in radio preventative maintenance services
- Maintaining and installing Authority radio systems, components and configuration
- Performing daily radio facility site and system checks
- Conducting FCC compliance activities
- Maintaining accurate radio system and equipment asset records
- Programming and configuring subscriber radios and encryption keys
- Monitoring system performance
- Performing analysis, troubleshooting, and solution delivery of radio networks issues
- Providing project and planning management
- Operating test equipment to examine systems
- Monitoring systems alarms and alerts 24 x 7
- Providing technical administration
- Conducting training
- Inspecting radio system technical work for compliance with standards and specifications
- Preparing technical documentation
- Interpreting blueprints, diagrams and schematics
- Attending meetings, conferences and events, as directed by the COTR
- Performing projects assigned by the COTR

Responsibilities: Support, oversight, and supervision of electronic equipment installation and maintenance. Perform basic system troubleshooting and repair activities. Provide support for portable, mobile, and fixed radios (control stations, base stations, and mobile relays), public address/siren, video equipment, communications consoles, and other related communications equipment.

Radio Maintenance Technician, (Page 2)

**Skills:** Maintain accurate computer system records, perform system equipment testing, maintain work records and accomplishments and other information as needed for station records. Use of basic hand and power tools. Measurement, layout, and attachment of equipment. Operation of basic electronic test equipment (Volt-Ohmeters, Wattmeters, Frequency Counters, Oscilloscopes, etc.) Customer service and user operation support. Microsoft Office Products (MS-Word, MS-Excel, MS-Access, MS-Outlook). Motorola CPS Programming and radio Template development. Ability to configure and program radio equipment. Performing Radio Firmware management and upgrades.

**Abilities:** Installs, tests, and repairs radio equipment. Able to follow moderate to complex instructions, both written and verbal. Able to prepare reports and documentation for work performed, and create and maintain accurate equipment service records.

**Required Education and Experience**

(10) Years of documented experience

High school graduate with electronics training, or associate's degree in electrical engineering technology

Installation and maintenance of land mobile radios and vehicle electrical systems.

**Required Certifications or Licensure:** FCC General Radio Operators License, CET or equivalent required

**Proficiency or Skills Testing Required:** Basic Installation Tools and Electrical Measurements. Soldering and RF connectorization. Excel, Land Mobile Radio practices.
APPENDIX F

CONTRACT SUPPLIED ITEMS – PARTIAL LIST
Appendix F – Contractor Supplied Items – Partial List

Hand Tools:
The Contractor shall acquire and assign the following (or functionally equivalent) hand tool sets to Contract employees in the following positions:

- Radio and Wireless Technical Services Coordinator
  - Tessco SKU # 56986
- Senior Radio Engineer
  - Tessco SKU # 56986
- Senior Network Engineer
  - Tessco SKU # 56986
- Supplemental Radiating System (SRS) Field Engineer
  - Tessco SKU # 56986
- Radio Frequency Engineering Planner
  - Tessco SKU # 56986
- System Analyst
  - Tessco SKU # 56986
- Senior Radio (Infrastructure) and Networking Technologist
  - Tessco SKU # 456879
- Field Radio Support Technician/Radio Communications Integration Technician
  - Tessco SKU # 56986
- Radio Maintenance Technician (2)
  - Tessco SKU # 56986

Safety/Work Clothing and Equipment (All Positions):

<table>
<thead>
<tr>
<th>Item</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pants</td>
<td>5 ea.</td>
<td>5.11 Tactical #74251 (M)/equal. Khaki or Dk. Navy #64359 (W)/equal. Dk. Navy</td>
</tr>
<tr>
<td>Shirt</td>
<td>5 ea.</td>
<td>5.11 Tactical #41060/equal. Dk Navy or Black</td>
</tr>
<tr>
<td>Jacket</td>
<td>1 ea.</td>
<td>5.11 Tactical #48017/equal. Dk Navy or Black</td>
</tr>
<tr>
<td>Hi-Vis Vest</td>
<td>1 each</td>
<td>ANSI 107-2010 Class II, Level II/ANSI 207-2006</td>
</tr>
<tr>
<td>Gloves</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hard Hat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hearing Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety Glasses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety Shoes (steel or composite toe)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX G

INFORMATION SECURITY STANDARD
INFORMATION SECURITY STANDARDS

FOREWORD

These Information Security Standards (ISS) define the Metropolitan Washington Airports Authority (the Authority) standards governing the set up and operation of all Authority owned data processing systems and associated networks. It is issued under the authority of the Authority Electronic Communications Systems Policy (GA-005), section 4.b.

George R. Ellis
Vice President for Information and Telecommunication Systems

Date 2/7/2011
## CONTENTS

1.0 Purpose .................................................................................................................. 1
2.0 Definitions ............................................................................................................. 1
3.0 Firewall Standard ................................................................................................. 2
4.0 Installation Standard for New Systems ................................................................. 3
5.0 Data Classification Standard ................................................................................ 3
6.0 Data Retention Standard ...................................................................................... 4
7.0 Encryption Standard ............................................................................................ 4
8.0 Vulnerability Management Standard .................................................................... 5
9.0 Patch Management Standard ................................................................................ 5
10.0 Access Control Standard .................................................................................... 5
11.0 Password Standard ............................................................................................ 6
12.0 Physical Security Standard ................................................................................ 7
13.0 Security Monitoring Standard ........................................................................... 8
14.0 Security Testing Standard .................................................................................. 9
15.0 Incident Response Standard ............................................................................... 10
16.0 Security Awareness Standard ............................................................................ 11
17.0 Vendor Management Standard .......................................................................... 11
18.0 Configuration Management Standard ................................................................ 12
19.0 Availability Management Standard ...................................................................... 12
1.0 Purpose

The Metropolitan Washington Airports Authority provides electronic communication equipment and systems to enable Users to accomplish the Authority's mission and to promote the efficient conduct of Authority business. It is consistent with the Authority's commitment to Safety, Security and Risk Reduction that standards be identified for the establishment, maintenance and usage of such systems in a manner that promotes Information Security.

This document is subordinate to, and is to be interpreted consistent with, the Authority Electronic Communications Systems Policy (GA-005). It is issued under the authority of the Authority Electronic Communications Systems Policy, section 4.b. and will be periodically reviewed, maintained and updated by the Office of Information and Telecommunications Systems.

2.0 Definitions

2.1 Authorized Personnel: See the Authority Electronic Communications Systems Policy (GA-005).

2.2 Confidential Information: See the Authority Electronic Communications Systems Policy (GA-005).

2.3 Information Security Group: A group within the Office of Information and Telecommunications Systems designated to monitor and improve the Authority's Information Security posture.

2.4 Network Architect: The person within the Office of Information and Telecommunications Systems designated as responsible for the design of the Authority Data Network.

2.5 Owner: See the Authority Electronic Communications Systems Policy (GA-005).

2.6 Private Information: See the Authority Electronic Communications Systems Policy (GA-005).

2.7 Policy: See the Authority Electronic Communications Systems Policy (GA-005).

2.8 System Custodian: See the Authority Electronic Communications Systems Policy (GA-005).

2.8.1 Database Custodian: A System Custodian who is tasked with the technical support of one or more databases.

2.8.2 Network Custodian: A System Custodian who is tasked with the technical support of network equipment and connections.

2.8.3 Server Custodian: A System Custodian who is tasked with the technical support of one or more servers.
2.8.4 Workstation Custodian: A System Custodian who is tasked with the technical support of one or more workstations and related peripheral devices.

2.9 User: See the Authority Electronic Communications Systems Policy (GA-005).

3.0 Firewall Standard

3.1 Firewall configuration standard

3.1.1 All firewall configurations will be tested and approved by the assigned Network Custodian.

3.1.2 The Network Custodian will update and maintain a network diagram with all connections into their assigned network represented and provide an updated copy to the Network Architect and to the Information Security Group within MA-600.

3.1.3 An enterprise firewall must be maintained at each Internet connection, between any demilitarized zone (DMZ) and the internal network zone and between network zones as determined by the Information Security Group.

3.1.4 The following individuals and/or groups have responsibilities for logical management of the listed network components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Responsible Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls</td>
<td>Network Custodian</td>
</tr>
<tr>
<td>Routers</td>
<td>Network Custodian</td>
</tr>
<tr>
<td>Switches</td>
<td>Network Custodian</td>
</tr>
<tr>
<td>Wireless Access Points</td>
<td>Network Custodian</td>
</tr>
<tr>
<td>VPN Devices</td>
<td>Network Custodian</td>
</tr>
<tr>
<td>IP Range Assignments</td>
<td>MA-640 (Network Architect)</td>
</tr>
</tbody>
</table>

Documentation of the approved settings of each firewall must be maintained by the Network Custodian.

3.1.5 Each protocol other than hypertext transfer protocol (HTTP), secure sockets layer (SSL), secure shell (SSH), hypertext transfer protocol over secure socket layer (HTTPS), transport layer security (TLS) and virtual private network (VPN) will be justified and documented by the Network Custodian.

3.1.6 Each protocol allowed, such as file transfer protocol (FTP), will be justified and documented by the Network Custodian with appropriate compensating controls.

3.1.7 Each Authority router will be configured according to the base rule set approved by the Network Custodian.

3.1.8 The Information Security Group will perform a quarterly review of firewall and router configuration files and compare to approved settings.
4.0 Installation Standard for New Systems

4.1 All vendor-supplied default passwords and accounts must be changed by the System Custodian as part of the system installation

4.1.1 For wireless environments, change wireless vendor defaults, including, but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable protected access technology for encryption and authentication according to current industry best practices.

4.2 New systems will be installed by the System Custodian according to industry best practices.

4.2.1 All unnecessary services and protocols will be disabled

4.2.2 System security parameters will be configured to prevent misuse

4.2.3 All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems and web servers will be removed

4.2.4 Each server will have only one primary function (for example, web server, database server, DNS, etc.)

4.3 Administrative access to systems across network boundaries will only be allowed by encrypted non-console services such as SSH, VPN or SSL

4.4 Warning banners will be displayed as specified in the Authority IT Policy – Banners as published on the Authority's Livelink site.

4.5 Screensavers that require re-verification will be enabled with no more than a 15 minute wait period.

5.0 Data Classification Standard

5.1 Any data containing information such as credit card data, social security numbers, performance issues or medical files is classified as private information

5.1.1 Private information must be protected by the information owner with the appropriate technical, administrative and physical safeguards

5.1.2 Private information may only be shared with authorized personnel, as determined by the information owner

5.1.3 Unauthorized disclosure or access to private information must be reported immediately to the immediate supervisor and/or information owner.

5.1.4 Private information may not be copied, moved, or stored onto local hard drives or removable electronic media without specific authorization by the information owner.

5.2 Any data containing information that is intended for Authority business purposes only, such as system information, pending procurement matters, Authority credit card data or prospective bond issues is classified as confidential
5.2.1 Confidential information must be protected by the information owner with the appropriate technical, administrative and physical safeguards.

5.2.2 Confidential information may only be shared with Authority employees and/or contractors on a business need-to-know basis, as determined by the information owner.

5.2.3 Unauthorized disclosure or access to confidential information must be reported immediately to the immediate supervisor and/or information owner.

6.0 Data Retention Standard

6.1 The System Owner will develop and assure implementation of data retention standards for information contained within their systems.

6.2 Data retention standards will be developed with full consideration to legal, regulatory and business requirements for retention of subject data.

6.3 Data retention standards will include provisions for disposal of data when no longer needed for legal, regulatory or business requirements.

6.4 Where legal, regulatory or business requirements dictate; a manual or automated process to remove data exceeding the applicable data retention standard will be developed.

7.0 Encryption Standard

7.1 Strong cryptography (as defined in FIPS 140-2) and security protocols will be used when transmitting private or confidential data such as passwords, pending procurement matters or credit card data.

7.1.1 When entering or transmitting private or confidential data such as passwords, pending procurement matters or credit card data via an Internet browser, you must ensure that the address begins with https:// and that the secure lock symbol is visible in your browser window.

7.1.2 Users must never transmit private or confidential data such as passwords, pending procurement matters or credit card data over an open, public network without encryption through security protocols such as secure sockets layer (SSLv3/TLS) and Internet protocol security (IPSEC).

7.1.3 Users must never send private or confidential data such as passwords, pending procurement matters or credit card data via unencrypted email or other unsecured methods.

7.1.4 Users must assure that the destination URL and/or IP number used in transmission of encrypted data is legitimate.
8.0 Vulnerability Management Standard
8.1 Anti-malware software will be deployed and maintained by the System Custodian on all systems commonly affected by viruses and other forms of malware
8.1.1 The software must be capable of detecting, removing and protecting against viruses and other forms of malicious software, including spyware and adware
8.2 The System Custodian will ensure, no less frequently than weekly, that all anti-malware mechanisms are current, actively running and capable of generating audit logs

9.0 Patch Management Standard
9.1 The System Custodian will ensure, no less frequently than monthly, that all system components and software have the latest vendor-supplied security patches installed
9.2 The System Custodian will maintain a method to identify newly discovered security vulnerabilities for Authority system components and software
9.3 All software development will follow a formal software development life cycle, implementing information security throughout the process
9.4 Separate development, test, and production environments will be maintained
9.5 There will be a separation of duties between production environments and others
9.6 There must be a documented change control process for all production hardware and software changes maintained by the System Custodian
9.7 The web application development teams will follow the Open Web Application Security Project guidelines during custom application development
9.8 All web-facing applications must be protected against known attacks by one of the following methods: (1) independent validation of all custom application code or (2) installing an application layer firewall in front of the web-facing application

10.0 Access Control Standard
10.1 Access to system components must be restricted on a business need-to-know basis
10.2 For usage of critical user-facing technologies, each user must abide by the standard/policy governing proper use, including:
10.2.1 Explicit management approval (See Electronic Communications Systems Policy, Sec. 5.b.)
10.2.2 Authentication/authorization for use of the technology as established by the System Custodian
10.2.3 Acceptable uses of the technologies (See Electronic Communications Systems Policy, Sec 9.a.)
10.2.4 Use only products from the company-approved list maintained by the System Custodian.
10.2.5 Automatic disconnect of sessions after a specific period of inactivity set by the System Custodian.
10.2.6 Activation of access for vendors only when needed, with immediate deactivation after use.

11.0 **Password Standard**

11.1 Username and password will be unique to an individual and not shared unless authorized by the System Custodian/Information Owner and the Information Security Group.

11.2 Where passwords are used, each System Custodian will maintain and enforce a password standard that meets or exceeds industry best practices and the Authority IT Policy – Passwords as published on the Authority’s Livelink site.

11.3 To access The Authority network remotely, each user must have two forms of authentication (such as a password and a VPN certificate).

11.4 Passwords must be encrypted during transmission and storage on all system components.

11.5 The System Custodian and/or Owner will ensure proper user authentication and password management on all system components as follows:

11.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.

11.5.2 Verify user identity before performing password resets.

11.5.3 Set network first-time passwords to a unique value for each user and change immediately after the first use.

11.5.4 Immediately revoke access for any terminated users.

11.5.5 Remove inactive user accounts at least every 90 days.

11.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed.

11.5.7 Communicate password procedures and policies to all users.

11.5.8 Do not use group, shared, or generic accounts and passwords, unless authorized by the System Custodian/Information Owner and the Information Security Group.

11.5.9 Change user passwords at least every 90 days.

11.5.10 Change administrative passwords at least every 60 days.

11.5.11 Require a minimum password length of at least eight characters.

11.5.12 Use passwords containing both numeric and alphabetic characters.

11.5.13 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
11.5.14 Limit repeated access attempts by locking out the user ID after not more than six attempts
11.5.15 Set the lockout duration to no less than thirty minutes or until an administrator enables the user ID
11.5.16 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal
11.5.17 Authenticate all access to any database containing private or confidential data. This includes access by applications, administrators, and all other users

12.0 Physical Security Standard

12.1 Facility entry controls will be implemented to limit and monitor physical access to areas containing private or confidential information
12.1.1 Cameras may be implemented to monitor such areas. Collected data may be monitored and must be stored for a minimum of seven days
12.1.2 Publicly accessible network jacks (other than those intended for guest usage) must require additional authentication before permitting any access
12.1.3 Access to wireless access points and wireless gateways must be restricted
12.1.4 Access to wireless handheld devices with access to private or confidential data must be restricted

12.2 Access to areas where private or confidential information is stored or transmitted must be restricted

12.3 Visitors entering areas where private or confidential data is processed or maintained:
12.3.1 Must be authorized by the system custodian
12.3.2 Must be escorted or given a temporary physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees
12.3.2.1 If a temporary physical token is given, it must be surrendered before leaving the facility or at the date of expiration

12.4 A visitors log that maintains a physical audit trail of visitor activity must be maintained. Collected data must be retained for a minimum of three months

12.5 Media back-ups must be stored in a secure location, preferably off-site

12.6 All paper and electronic media that contains private or confidential data must be physically secured

12.7 The internal and external distribution of any kind of media that contains private or confidential data must be strictly controlled
12.7.1 Mark the media as private or confidential
12.7.2 Transfer the media by secured courier or other delivery method that can be accurately tracked

12.8 Management must approve any and all media that is moved from a secured area, especially when media is distributed to individuals

12.9 The storage and accessibility of media that contains private or confidential data must be strictly controlled

12.9.1 All such media must be properly inventoried and securely stored

12.10 Once the decision to destroy media containing private or confidential data has been made, destruction must proceed as follows:

12.10.1 Cross-cut shred, incinerate or pulp hardcopy materials

12.10.2 Purge, degauss, shred or otherwise destroy electronic media so that private or confidential data cannot be reconstructed

13.0 Security Monitoring Standard

13.1 The System Custodian will ensure that all access to system components are linked to each individual user for logging purposes.

13.2 The System Custodian will ensure that automated audit trails for all system components are implemented to reconstruct the following events:

13.2.1 All individual user accesses to private or confidential data (through the application or otherwise)

13.2.2 All actions taken by any individual with root or administrative privileges

13.2.3 Access to audit trails of financial systems or other systems primarily used to process and store private or confidential data

13.2.4 Invalid logical access attempts

13.2.5 Use of application level identification and authentication mechanisms

13.3 The System Custodian will ensure that all audit trail entries record at least the following parameters for each event:

13.3.1 User identification

13.3.2 Type of event

13.3.3 Date and time

13.3.4 Success or failure indication

13.3.5 Origination of event

13.3.6 Identity or name of affected data, system component, or resource.

13.4 The System Custodian will ensure that all critical system clocks and times are synchronized

13.5 The System Custodian will ensure that all audit trails are secured so that they cannot be altered, and:

13.5.1 Limit viewing of audit trails to those with a job-related need

13.5.2 Protect audit trail files from unauthorized modifications

13.5.3 Promptly back-up audit trail files to a centralized log server or media that is difficult to alter
13.5.4 Copy logs for wireless networks onto a log server on the internal LAN.

13.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert) if a centralized log server is not being used.

13.6 The System Custodian will review logs for all system components at least daily or implement an automated log reviewing function that will generate alerts for unusual events. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol servers (for example, RADIUS).

13.7 Audit trail history must be retained for at least two years, with a minimum of three months online availability.

13.8 The System Custodian will monitor and analyze security alerts and information and distribute to appropriate personnel (including the Information Security Group).

14.0 Security Testing Standard

14.1 The System Custodian (or Information Security Group if designated by the System Custodian) will test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts.

14.2 The System Custodian (or Information Security Group if designated by the System Custodian) will test wireless access security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts.

14.3 The System Custodian (or Information Security Group if designated by the System Custodian) will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). At a minimum, quarterly external vulnerability scans must be performed by an approved scanning vendor certified by the PCI Security Standards Council.

14.4 The System Custodian (or Information Security Group if designated by the System Custodian) will perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:

14.4.1 Network-layer penetration tests

14.4.2 Application-layer penetration tests.

14.5 The System Custodian (or Information Security Group if designated by the System Custodian) will use network intrusion detection systems and/or
host-based intrusion detection systems and/or intrusion prevention systems to monitor network traffic and alert personnel to suspected compromises. The System Custodian or Information Security Group will ensure that all intrusion detection and prevention engines are up-to-date.

15.0 Incident Response Standard

15.1 Members of the Computer Incident Response Team are as follows:
   15.1.1 The Information Security Group
   15.1.2 MA-610 Managers
   15.1.3 All System Custodians
   15.1.4 Others, as needed.

15.2 Authority system users shall notify the Computer Incident Response Team of all potential security incidents, including but not limited to:
   15.2.1 Unauthorized use; (sending SPAM, chain e-mails or threatening e-mails, planting viruses, conducting network-level probes/scans, exceeding authorization level, etc.)
   15.2.2 Theft of data
   15.2.3 Unauthorized alteration or deletion of data
   15.2.4 Denial of service and/or system failure
   15.2.5 Unsuccessful access attempts repeated in excess of defined thresholds
   15.2.6 Unauthorized access that is manifested:
      15.2.6.1 Internally (by an employee, customer, vendor or other on company property)
      15.2.6.2 Externally (by an employee, customer, vendor and all others outside company property)

15.3 The Computer Incident Response Team shall establish procedures to:

15.3.1 Recover systems or services as quickly as possible
15.3.2 Analyze and identify the cause of the incident
   15.3.2.1 Allowing only clearly identified and authorized staff to access live data and systems
   15.3.2.2 Document in detail all emergency actions
   15.3.2.3 Report to management all emergency actions
   15.3.2.4 Confirm the integrity of business systems and security controls with minimal delay
15.3.3 Plan and implement remedies to prevent recurrence
15.3.4 Collect audit trails and/or evidence
   15.3.4.1 To provide evidence for investigation, prosecution, and disciplinary actions, certain information should be captured whenever it is suspected that computer or network related crime or abuse has taken place
15.3.4.2 The relevant information should be securely stored off-line until such time as it is determined that The Authority will not pursue legal action or otherwise use the information.

15.3.4.3 The information to be immediately collected includes the system logs, application audit trails, other indications of the current system states, as well as copies of all potentially involved files.

15.3.5 Communicate with business users and others affected by or involved with the recovery from the incident.

16.0 Security Awareness Standard

16.1 All Authority users will attend at least one hour of Information Security training each year.

16.2 Security related articles/inserts will appear in each monthly issue of IT's NEWS.

17.0 Vendor Management Standard

17.1 Contracting Officers and Contracting Officers' Technical Representatives will exercise due diligence in selecting IT outsourcing service providers.

17.2 Contracting Officers and Contracting Officers’ Technical Representatives will require IT outsourcing service providers by contract to implement appropriate measures designed to meet the objectives below:

17.2.1 Ensure the security and confidentiality of private and confidential information.

17.2.2 Protect against any anticipated threats or hazards to the security or integrity of such information.

17.2.3 Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any entity.

17.2.4 Dispose of private and confidential information in a secure manner.

17.2.5 Immediately inform The Authority in the event of a security breach involving private or confidential information.

17.3 Contracting Officers’ Technical Representatives will monitor IT outsourcing service providers to confirm that they have satisfied the obligations described above. As part of this monitoring, Contracting Officers and Contracting Officers’ Technical Representatives will review documents that may include, but are not limited to, contracts, audits, and summaries of test results or other documents. In addition, Contracting Officers and Contracting Officers’ Technical Representatives will request a SAS 70 Part II or equivalent third-party assessment of significant IT outsourcing service providers. These reviews will take place on at least an
annual basis for existing vendors. For new vendors, these documents will be reviewed prior to signing any contract.

18.0 Configuration Management Standard

18.1 System Custodian will maintain an inventory of information system components (hardware and software) under their control that:

18.1.1 Ensures the security and confidentiality of private and confidential information

18.1.2 Accurately reflects the current information system(s);

18.1.3 Is consistent with the authorized boundary of the information system(s);

18.1.4 Is at a level of granularity necessary for tracking and reporting.

19.0 Availability Management Standard

19.1 System Custodian will take all reasonable steps to assure system availability during required hours of operation. Steps shall include:

19.1.1 Providing adequate HVAC for equipment;

19.1.2 Providing adequate power supply and power conditioning for equipment;

19.1.3 Performing periodic backups of all central production servers;

19.1.4 Performing periodic restoration testing of central production servers;

19.2 Review, no less frequently than annually, the system architecture (redundant hardware, data paths, and power) for appropriateness.
APPENDIX H

PSWN BEST PRACTICES
Operational Best Practices for Managing Trunked Land Mobile Radio Systems

Final

May 2003
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. INTRODUCTION ..................................................................</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Scope ...........................................................................</td>
<td>1</td>
</tr>
<tr>
<td>1.3 Background ....................................................................</td>
<td>2</td>
</tr>
<tr>
<td>1.4 Document Organization ................................................................</td>
<td>2</td>
</tr>
<tr>
<td>2. METHODOLOGY ....................................................................</td>
<td>4</td>
</tr>
<tr>
<td>3. KEY CONSIDERATIONS OVERVIEW .........................................</td>
<td>5</td>
</tr>
<tr>
<td>4. BEST PRACTICES ASSESSMENT ............................................</td>
<td>7</td>
</tr>
<tr>
<td>4.1 Technical Best Practices .............................................</td>
<td>8</td>
</tr>
<tr>
<td>4.2 Operational Best Practices ...........................................</td>
<td>12</td>
</tr>
<tr>
<td>4.2.1 Talk Group Organization ..........................................</td>
<td>13</td>
</tr>
<tr>
<td>4.2.2 System Administration .............................................</td>
<td>14</td>
</tr>
<tr>
<td>4.2.3 Interoperability ....................................................</td>
<td>17</td>
</tr>
<tr>
<td>4.2.4 Training ....................................................................</td>
<td>19</td>
</tr>
<tr>
<td>4.3 Political Best Practices ..............................................</td>
<td>21</td>
</tr>
<tr>
<td>5. LESSONS LEARNED ASSESSMENT ..........................................</td>
<td>23</td>
</tr>
<tr>
<td>6. CONSIDERATIONS AND CONCLUSIONS ......................................</td>
<td>28</td>
</tr>
<tr>
<td>APPENDIX A—TRUNKING OVERVIEW ...........................................</td>
<td>A-1</td>
</tr>
<tr>
<td>APPENDIX B—DATA COLLECTION MATERIALS ...................................</td>
<td>B-1</td>
</tr>
<tr>
<td>APPENDIX C—OPERATING ENVIRONMENT OVERVIEW ............................</td>
<td>C-1</td>
</tr>
<tr>
<td>APPENDIX D—KEY TECHNICAL CONSIDERATIONS ................................</td>
<td>D-1</td>
</tr>
<tr>
<td>D.1 Capacity .......................................................................</td>
<td>1</td>
</tr>
<tr>
<td>D.2 Security .......................................................................</td>
<td>1</td>
</tr>
<tr>
<td>D.3 Trunking Protocols .....................................................</td>
<td>3</td>
</tr>
<tr>
<td>APPENDIX E—KEY OPERATIONAL CONSIDERATIONS ............................</td>
<td>E-1</td>
</tr>
<tr>
<td>E.1 Talk Group Organization ..............................................</td>
<td>1</td>
</tr>
<tr>
<td>E.2 System Administration ..................................................</td>
<td>4</td>
</tr>
<tr>
<td>E.3 Interoperability ..........................................................</td>
<td>8</td>
</tr>
<tr>
<td>E.4 Training .......................................................................</td>
<td>12</td>
</tr>
<tr>
<td>APPENDIX F—KEY POLITICAL ARENA CONSIDERATIONS ....................</td>
<td>F-1</td>
</tr>
<tr>
<td>F.1 Coordination ...................................................................</td>
<td>1</td>
</tr>
<tr>
<td>F.2 Resource Sharing .......................................................</td>
<td>2</td>
</tr>
<tr>
<td>F.3 Stakeholder Support .....................................................</td>
<td>2</td>
</tr>
<tr>
<td>APPENDIX G—PROJECT 25 ........................................................</td>
<td>G-1</td>
</tr>
<tr>
<td>APPENDIX H—LIST OF ACRONYMS ............................................</td>
<td>H-1</td>
</tr>
</tbody>
</table>
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 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>
<thead>
<tr>
<th>System Size</th>
<th>Radio User Population</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>Fewer than 5,000</td>
</tr>
<tr>
<td>Medium</td>
<td>5,000—10,000</td>
</tr>
<tr>
<td>Large</td>
<td>More than 10,000</td>
</tr>
</tbody>
</table>

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](image)

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

**Technical Environment**

![Technical Environment Diagram](image)

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

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

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Political</td>
<td>• Participate in working groups</td>
</tr>
<tr>
<td></td>
<td>• Share resources</td>
</tr>
<tr>
<td></td>
<td>• Garner stakeholder and user acceptance</td>
</tr>
</tbody>
</table>

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

**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 multi-story 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

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

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Talk Group</td>
<td>• Involve the user community in planning</td>
</tr>
<tr>
<td>Organization</td>
<td>• Define a default fleet map</td>
</tr>
<tr>
<td></td>
<td>• Develop a standardized template across domains</td>
</tr>
<tr>
<td></td>
<td>• Regularly review fleet maps and talk group plans</td>
</tr>
</tbody>
</table>

- **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>
<thead>
<tr>
<th>Consideration</th>
<th>Best Practices</th>
</tr>
</thead>
</table>
| **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**

<table>
<thead>
<tr>
<th>Interoperability</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>• Implement special operations or coordination talk groups</strong></td>
<td></td>
</tr>
<tr>
<td><strong>• Match unit numbers and zones when sharing subscriber IDs in a region</strong></td>
<td></td>
</tr>
<tr>
<td><strong>• Consider transportable interoperability solutions to address commercial interference</strong></td>
<td></td>
</tr>
</tbody>
</table>
• **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>
<thead>
<tr>
<th>Consideration</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training</td>
<td>• Establish training teams</td>
</tr>
<tr>
<td></td>
<td>• Survey users to identify systems concerns</td>
</tr>
<tr>
<td></td>
<td>• Develop multiple training delivery formats</td>
</tr>
<tr>
<td></td>
<td>• Employ visual aids</td>
</tr>
</tbody>
</table>

- **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>
<thead>
<tr>
<th>Consideration</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Political</td>
<td>• Participate in working groups</td>
</tr>
<tr>
<td></td>
<td>• Share resources</td>
</tr>
<tr>
<td></td>
<td>• Garner stakeholder and user acceptance</td>
</tr>
</tbody>
</table>

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

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

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 choose 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.**

  The 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](image-url)
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

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

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
I. Contact/Demographic Information

1. Please provide the following information.

<table>
<thead>
<tr>
<th>Name</th>
<th>Position and Division</th>
<th>Agency Name and Mailing Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone/Fax Number</th>
<th>E-Mail/Web Address</th>
<th>May we contact you in the future? (If “Yes,” indicate any restrictions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(P)</td>
<td>@</td>
<td>☐ Yes: _________________________ ☐ No</td>
</tr>
<tr>
<td>(F)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Number of Radio Users</th>
<th>Number of Stations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law Enforcement Agencies</td>
<td></td>
</tr>
<tr>
<td>Fire Departments</td>
<td></td>
</tr>
<tr>
<td>EMS Agencies</td>
<td></td>
</tr>
</tbody>
</table>
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).

<table>
<thead>
<tr>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>□ Motorola □ GE □ M/A-Com (Ericsson) □ EF Johnson □ MA-Com (Open Sky)</td>
</tr>
<tr>
<td></td>
<td>□ Other (specify)</td>
</tr>
<tr>
<td>Model</td>
<td>□ EDACS □ LTR □ MPT 1327 □ Project 25 □ SmartNet □ SmartZone □ Open Sky</td>
</tr>
<tr>
<td></td>
<td>□ Other (specify)</td>
</tr>
<tr>
<td>What type of trunking protocol is used?</td>
<td>□ Transmission</td>
</tr>
<tr>
<td></td>
<td>□ Message</td>
</tr>
<tr>
<td>What type of database management software is used?</td>
<td></td>
</tr>
<tr>
<td>Installer</td>
<td>□ In-house □ Manufacturer □ Electronics Shop</td>
</tr>
<tr>
<td></td>
<td>□ Other (specify)</td>
</tr>
<tr>
<td>Band (MHz)</td>
<td>□ 138–144/148–174 □ 406–420</td>
</tr>
<tr>
<td></td>
<td>□ 450–470</td>
</tr>
<tr>
<td></td>
<td>□ Other (specify)</td>
</tr>
<tr>
<td>Approximate System Age</td>
<td></td>
</tr>
<tr>
<td>Encryption Capable?</td>
<td>□ Yes □ No</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model</th>
<th>Quantity</th>
<th>Approximate Age</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model</th>
<th>Quantity</th>
<th>Approximate Age</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9. Please describe console equipment.

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model</th>
<th>No. of Control Channels</th>
<th>No. of Dispatch Positions</th>
<th>Location (address)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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?

<table>
<thead>
<tr>
<th>Types of PTTs</th>
<th>Average Number of PTTs/Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile-to-mobile</td>
<td></td>
</tr>
<tr>
<td>Private</td>
<td></td>
</tr>
<tr>
<td>Emergency</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td></td>
</tr>
<tr>
<td>Dispatch</td>
<td></td>
</tr>
<tr>
<td>Telephone interconnect</td>
<td></td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Agency</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geographical Region</td>
<td>Suburban</td>
<td>Suburban</td>
<td>Suburban</td>
<td>Metropolitan</td>
<td>Metropolitan/ Suburban</td>
<td>Suburban</td>
<td>Suburban/ Rural</td>
<td>Metropolitan/ Suburban</td>
<td>Metropolitan/ Suburban</td>
<td>Metropolitan</td>
<td>Suburban</td>
<td>Rural</td>
</tr>
<tr>
<td>User Population</td>
<td>Small</td>
<td>Small</td>
<td>Medium</td>
<td>Medium</td>
<td>Large</td>
<td>Large</td>
<td>Large</td>
<td>Large</td>
<td>Large</td>
<td>Large</td>
<td>Medium</td>
<td>Small</td>
</tr>
<tr>
<td>User Domain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Fire/EMS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Public Works</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>N/A</td>
<td>N/A</td>
<td>✓</td>
</tr>
<tr>
<td>Age (years)</td>
<td>&gt; 10</td>
<td>&gt; 10</td>
<td>&lt; 5</td>
<td>&lt; 5</td>
<td>&lt; 5</td>
<td>6 to 10</td>
<td>6 to 10</td>
<td>&lt; 5</td>
<td>&gt; 10</td>
<td>&lt; 5</td>
<td>6 to 10</td>
<td>&gt; 10</td>
</tr>
<tr>
<td>Mode of Operation</td>
<td>Mixed</td>
<td>Analog</td>
<td>Digital</td>
<td>Digital</td>
<td>Digital</td>
<td>Mixed</td>
<td>Analog</td>
<td>Analog</td>
<td>Analog</td>
<td>Analog</td>
<td>Analog</td>
<td></td>
</tr>
<tr>
<td>Trunking Protocol</td>
<td>Transmission</td>
<td>Unknown</td>
<td>Transmission</td>
<td>Message</td>
<td>Transmission</td>
<td>Transmission</td>
<td>Transmission</td>
<td>Unknown</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption Capable</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>No</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Number of Talk Groups</td>
<td>40</td>
<td>40</td>
<td>238</td>
<td>212</td>
<td>150</td>
<td>350</td>
<td>253</td>
<td>1,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Talk Group Organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fleet Map Planning Participants</td>
<td>Unknown (limited documentation exists)</td>
<td>Vendor</td>
<td>Limited agency participation</td>
<td>Agency specific user groups</td>
<td>Vendor representatives</td>
<td>LMR consultants</td>
<td>Surveyed all participating organizations</td>
<td>Vendor representatives</td>
<td>Command staff</td>
<td>Radio technical supervisor</td>
<td>Limited documentation exists</td>
<td>Major study to release RFP</td>
</tr>
<tr>
<td>Predefined Fleet Map</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>None</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assigned User Priority</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Performance Monitoring</td>
<td>Ad hoc</td>
<td>No</td>
<td>No</td>
<td>Ad hoc</td>
<td>Monthly</td>
<td>Monthly</td>
<td>Ad hoc</td>
<td>Daily</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subscriber ID Management</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster Plan</td>
<td>None</td>
<td>None</td>
<td>✓</td>
<td>None</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Future Growth Plan</td>
<td>Limited</td>
<td>✓</td>
<td>Limited</td>
<td>None</td>
<td>None</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Maintenance</td>
<td>Agency</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
<td>G</td>
<td>H</td>
<td>I</td>
<td>J</td>
<td>K</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
<td>--------</td>
<td>---------</td>
<td>---------</td>
<td>----</td>
<td>-----</td>
<td>-----------</td>
<td>---------</td>
<td>-----</td>
<td>---------------</td>
<td>----------</td>
<td>----</td>
</tr>
<tr>
<td>In-House or Outsourced</td>
<td>Outsource</td>
<td>Outsource</td>
<td>Mixed</td>
<td>In House</td>
<td>In House</td>
<td>Mixed</td>
<td>In House</td>
<td>Mixed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proactive or Responsive</td>
<td>Responsive</td>
<td>Responsive</td>
<td>Proactive</td>
<td>Proactive</td>
<td>Proactive</td>
<td>Proactive</td>
<td>Proactive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Failure Tests</td>
<td>None</td>
<td>None</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>None</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Solution</td>
<td>Blue</td>
<td>Maroon</td>
<td>Green</td>
<td>Not applicable</td>
<td>Blue</td>
<td>Blue</td>
<td>Diamond</td>
<td>Blue</td>
<td>Blue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Solution</td>
<td>Blue</td>
<td>Maroon</td>
<td>Grey</td>
<td>Not applicable</td>
<td>Blue</td>
<td>Blue</td>
<td>Triangle</td>
<td>Blue</td>
<td>Blue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regional Solution</td>
<td>Red</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Not applicable</td>
<td>Blue</td>
<td>Blue</td>
<td>Diamond</td>
<td>Blue</td>
<td>Blue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Federal Solution</td>
<td>Red</td>
<td>Yellow</td>
<td>Red</td>
<td>Not applicable</td>
<td>Blue</td>
<td>Blue</td>
<td>Diamond</td>
<td>Blue</td>
<td>Blue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P25 Compliant</td>
<td>No</td>
<td>No</td>
<td>✓</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Participate in Regional Working Groups</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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
- NPS PAC
- ▼ 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.

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.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{message_trunking.eps}
\caption{Message Trunking versus Transmission Trunking\(^6\)}
\end{figure}

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](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, 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**

![System Maintenance Diagram]

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 section 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.

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

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

PSWN RECOMMENDED SECURITY POLICY
Land Mobile Radio System
Recommended Security Policy

FINAL

October 1999
FOREWORD

This document, presented by the Public Safety Wireless Network (PSWN) program, outlines a recommended security policy for public safety agencies. Public safety agencies may apply this security policy to the design, implementation, and operation of their land mobile radio (LMR) systems. If this policy is implemented and followed, it should improve the overall system security of current and developing public safety LMR systems.

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 BACKGROUND</td>
<td>1</td>
</tr>
<tr>
<td>1.2 PURPOSE</td>
<td>2</td>
</tr>
<tr>
<td>1.3 SCOPE</td>
<td>2</td>
</tr>
<tr>
<td>1.4 DOCUMENT ORGANIZATION</td>
<td>2</td>
</tr>
<tr>
<td>2. SECURITY POLICY</td>
<td>3</td>
</tr>
<tr>
<td>2.1 ADMINISTRATIVE SECURITY</td>
<td>3</td>
</tr>
<tr>
<td>2.1.1 Security Plans, Procedures, and Documentation</td>
<td>3</td>
</tr>
<tr>
<td>2.1.2 Contingency Plans</td>
<td>4</td>
</tr>
<tr>
<td>2.1.3 Security Awareness and Training</td>
<td>4</td>
</tr>
<tr>
<td>2.1.4 System Development and Maintenance</td>
<td>4</td>
</tr>
<tr>
<td>2.1.5 Configuration Management</td>
<td>5</td>
</tr>
<tr>
<td>2.1.6 Software and Data Security</td>
<td>5</td>
</tr>
<tr>
<td>2.1.7 Personnel Security</td>
<td>6</td>
</tr>
<tr>
<td>2.2 PHYSICAL SECURITY</td>
<td>6</td>
</tr>
<tr>
<td>2.3 COMPUTER SECURITY</td>
<td>6</td>
</tr>
<tr>
<td>2.3.1 Authentication</td>
<td>7</td>
</tr>
<tr>
<td>2.3.2 Access Control</td>
<td>7</td>
</tr>
<tr>
<td>2.3.3 Audit</td>
<td>7</td>
</tr>
<tr>
<td>2.3.4 Object Reuse</td>
<td>8</td>
</tr>
<tr>
<td>2.4 COMMUNICATIONS SECURITY</td>
<td>8</td>
</tr>
<tr>
<td>2.4.1 Transmission Security</td>
<td>8</td>
</tr>
<tr>
<td>2.4.2 Encryption</td>
<td>8</td>
</tr>
<tr>
<td>2.4.3 Key Management</td>
<td>10</td>
</tr>
<tr>
<td>2.4.4 Firewall</td>
<td>10</td>
</tr>
<tr>
<td>2.5 RADIO SECURITY</td>
<td>10</td>
</tr>
<tr>
<td>2.6 MOBILE DATA TERMINAL/MOBILE COMPUTER TERMINAL SECURITY</td>
<td>11</td>
</tr>
<tr>
<td>APPENDIX A—REFERENCES</td>
<td>A-1</td>
</tr>
<tr>
<td>APPENDIX B—GLOSSARY</td>
<td>B-1</td>
</tr>
<tr>
<td>APPENDIX C—ACRONYMS</td>
<td>C-1</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

Protecting emergency services infrastructure, which includes public safety organizations and their communications systems, presents many challenges for policy makers who influence information technology systems and for the public safety community. Many authorities—Executive Order 13010, National Partnership for Reinventing Government (NPRG) Action Item A06 formerly known as National Performance Review, the final report from the President’s Commission on Critical Infrastructure Protection (PCCIP), and Presidential Decision Directives (PDD) 62 and 63—require that the emergency services infrastructure be protected from physical and cyber threats. The Public Safety Wireless Network (PSWN) Program Management Office (PMO) supports this ongoing requirement by encouraging public safety agencies to prepare for major technology changes that could dramatically affect the security of their communications systems.

This document outlines a recommended security policy that local, state, and federal public safety agencies may use throughout their land mobile radio (LMR) communications systems’ life cycle. Security policy is defined as the set of regulations, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. This security policy can serve as a model for agencies when developing their individual security policies.

1.1 Background

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

Threats are intentional or unintentional actions taken against a system that can result in the modification, disclosure, or destruction of sensitive or private information or that can degrade or disable system operations. Security vulnerabilities are weaknesses in a system’s protection schemes that may be exploited. The degree of risk associated with a system depends on the likelihood of a threat being carried out and the severity of associated vulnerabilities. Candidates that have been proposed as new LMR standards address security controls to some extent, yet many do not address minimizing the vulnerability of radio systems to computer-based threats.

The PSWN Digital Land Mobile Radio Risk Assessment Report, dated January 1998, provides a preliminary security threat and vulnerability assessment of LMR security standards. This assessment emphasizes the generic system model as defined in the Telecommunications
Industry Association/Electronics Industry Association (TIA/EIA) Interim Standards (IS) and Telecommunications Systems Bulletins (TSB) 102 series documents. The risk assessment finds LMR security standards deficient in a number of areas, including authentication, access control, and accountability. These deficiencies result in a host of potential vulnerabilities. The assessment reveals heavy reliance on encryption for confidentiality of communications, rather than the use of AIS-based security features for total system security.

The *PSWN Digital Land Mobile Radio Security Guidelines Recommendations*, dated October 1998, forms the basis for this document and recommends a common set of security guidelines for public safety LMR systems. Establishing security guidelines is considered a critical first step in ensuring the incorporation of adequate security controls and best security practices in public safety LMR systems.

### 1.2 Purpose

This document provides a recommended security policy for public safety LMR systems. The PSWN program believes that establishing a communications system security policy is a critical first step in ensuring that adequate security controls and best security practices are made a part of the development of new public safety LMR systems.

### 1.3 Scope

The policy outlined in this document is applicable to planned and operational public safety LMR systems. It addresses areas of administrative security, physical security, computer security, communications security, radio security, and mobile computer terminals (MCT) and mobile data terminals (MDT) as they relate to LMR systems. This security policy has been formulated in accord with a variety of sources, including federal government security policies and industry best security practices.

### 1.4 Document Organization

The remainder of this document is organized as follows:

- Section 2, Security Policy—Definition of security policies for administrative, physical, computer, communications, radio, and MCT/MDT security
- Appendix A—Reference list of security guidelines sources
- Appendix B—Glossary
- Appendix C—Acronyms.
1. SECURITY POLICY

This section defines the recommended radio system security policy in the following areas:

- Administrative security
- Physical security
- Computer security
- Communications security
- Radio security
- MCT/MDT security.

Addressing security in all of these areas is critical because vulnerabilities in any area may negate the effectiveness of security controls in the other areas.

2.1 Administrative Security

Administrative security employs established procedural controls to ensure the confidentiality, integrity, and availability of the LMR system. Administrative security is important regardless of the technology employed. Existing analog LMR systems as well as evolving, computer-based LMR systems should have solid administrative security programs. Administrative security policy consists of policy statements about security documentation, security training, system development life-cycle controls, and personnel security.

2.1.1 Security Plans, Procedures, and Documentation

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

1. A security program, including security plans, procedures, and other documented security safeguards, shall be put in place to meet all rules, regulations, and practices that direct how an agency manages, protects, and distributes sensitive information and communications.

2. Security-related activities (e.g., risk assessments and security testing) shall be conducted to ensure that the security plans and procedures are effective. The results of the security activities shall be documented.
2.1.2 Contingency Plans

The policy requires contingency plans to provide directions for emergency response, backup operations, and post-disaster recovery, should an emergency or disaster occur. The contingency plan policy is as follows:

1. Contingency and disaster recovery plans shall be developed that detail continuity of operations and alternative-site arrangements.

2. Contingency plans shall be tested to ensure that they effectively provide the capability to continue service based on system needs and priorities.

3. Contingency plans shall be updated regularly to ensure that they provide continuity of operations for the agency at all times.

4. Adequate alternative paths shall be available to transmit information.

2.1.3 Security Awareness and Training

Security awareness and training is a continual process that educates all individuals in an agency about its security policy, including best security practices and procedures. Security training can be conducted through scheduled programs or through memorandums and brochures. The security awareness and training policy is as follows:

1. Security training shall be provided to all personnel (i.e., agency employees and contractors) who will use or manage the system.

2. Security training shall include radio- and system-related threats and emergency operations.

3. Periodic refresher training shall be provided for each group of users.

4. An ongoing awareness program shall be provided to ensure that all users are kept aware of both old and new threats to the system.

2.1.4 System Development and Maintenance

The system development and maintenance policy ensures the integrity of the system throughout the system life cycle. Further, the policy ensures that all system software is developed and maintained with the concurrence of authorized personnel. The system development and maintenance policy is as follows:

1. System software shall be developed and maintained only with the concurrence of authorized personnel and through the direct access by authorized personnel.
2. Software shall be developed in a controlled, secure environment.

3. Software developed in a controlled environment shall be delivered to user sites via authorized carriers.

2.1.5 Configuration Management

The configuration management policy deals with the control of changes made to a system’s hardware, software, firmware, documentation, tests, test fixtures, and test documentation throughout the development and operational life of the system. This control is necessary to prevent changes that could negatively affect the security posture of the radio system unless managers are at least aware of potential risks. The configuration management policy is as follows:

1. Managers shall ensure that proper configuration control begins in the earliest stages of system design and development and that it extends over the full life of the system.

2. A configuration management system shall be used to control and document every change made to software and applications.

3. All changes made to documentation, hardware, or software shall be reviewed and approved by a designated security official.

4. Software version controls shall be implemented.

2.1.6 Software and Data Security

Radio system managers need to ensure the integrity, confidentiality, and availability of the software that controls their systems’ operation and the data the systems process. Therefore, procedural safeguards should be established to protect the software and data from accidental or deliberate modification, destruction, or disclosure. The software and data security policy is as follows:

1. Object and source code for system software shall be securely stored when not in use by the developer.

2. All software development activities shall take place in a controlled facility.

3. Source code shall not be delivered to users.

4. Sensitive data stored on removable media shall be placed in an appropriately controlled container or facility.

5. Critical data shall be backed up regularly and the backup media (e.g., diskettes, tapes) shall be stored in a secure environment.
2.1.7 Personnel Security

The personnel security policy ensures that all personnel (i.e., agency employees and contractors) with access to the system have the proper need to know for information to which they have access. It also ensures that users with special privileges (e.g., system administrators) are properly investigated before they are given access to the system. The personnel security policy is as follows:

1. All personnel who have access to the system shall have proper need to know information to which they have access.

2. Individuals shall undergo a background investigation before being placed in critical sensitive positions or authorized to bypass significant technical and security controls on the system.

3. All routine, on-site maintenance functions shall be performed by hardware and systems software specialists who have been cleared to the highest level of information processed by the system.

2.2 Physical Security

The physical security policy addresses the protection of communications equipment and facilities that house the equipment. Facilities may include buildings housing communications centers, network management systems, remote tower sites, dispatch centers, and maintenance facilities. This policy addresses facility security and environmental protection. The physical security policy is as follows:

1. Physical security controls shall be implemented at all sites, including the following:
   a) Access controls for facilities (e.g., electronic access devices, keys, guards)
   b) Proper visual identification of employees and visitors (i.e., badges)
   c) Restriction of access for all unauthorized personnel
   d) Additional access controls for computer and telecommunications rooms
   e) Additional access controls for rooms that house file servers.

2. Proper environmental controls (e.g., air conditioning, uninterruptible power supply) shall be provided as appropriate for each facility.

2.3 Computer Security

A significant feature of evolving LMR systems is the increasing extent to which the radio systems are managed by computerized means. Interfaces between system components are also increasingly likely to occur via network connections.

Computer security is the aspect of security that focuses on computer hardware and software, their use, and networking components. The following subsections describe the four
basic components of computer security (i.e., authentication, access control, audit, and object reuse) and how these relate to LMR systems.

2.3.1 Authentication

The authentication policy ensures that only authorized personnel have access to the system and the information processed by the system. The authentication policy is as follows:

1. *The proper controls shall be in place to authenticate the identity of users in accord with any access control policies and to validate each user’s authorization before allowing the user to access information or services on the system.*

2. *User account management shall be in place to ensure that only valid users are able to access the information or services on the system.*

3. *Authentication data shall be protected from unauthorized access.*

2.3.2 Access Control

The access control policy protects LMR information, services, and resources from unauthorized access or tampering. The access control policy is as follows:

1. *Controls shall be in place to ensure that only personnel with the proper authorization and a need to know are granted access to LMR systems and their resources.*

2. *Critical system services and resources shall be protected from unauthorized use.*

3. *Remote access shall be controlled through identification and authentication mechanisms and restricted to a limited number of authorized personnel.*

2.3.3 Audit

The audit policy ensures that all users are held accountable for their actions and that attempted and actual security violations are detected. The audit policy is as follows:

1. *The system shall create, maintain, and protect an audit trail of security-related events (e.g., log-on, log-off, access to system administrator functions).*

2. *The security-related events shall be traceable to the user or process responsible for initiating the event.*

3. *Procedures shall be in place for the regular review of audit data by authorized personnel.*
2.3.4 Object Reuse

The object reuse policy safeguards the confidentiality of information stored in the LMR system and protects it from unauthorized access. The object reuse policy is as follows:

1. Storage media containing sensitive information shall be completely empty before reassigning that medium to a different user.

2.4 Communications Security

The communications security policy goal is to ensure the confidentiality and integrity of information transmitted among the LMR system components. Communications security includes transmission security, encryption, key management, and firewall. Policies for each of these areas are provided below. [Refer to the Glossary in Appendix B for definitions of terms used in this section.]

2.4.1 Transmission Security

The transmission security policy is designed to protect transmissions from interception and exploitation by means other than cryptoanalysis and from jamming. The transmission policy is as follows:

1. Controls other than encryption (e.g., frequency-hopping, spread spectrum) shall be in place to provide communications transmissions adequate protection from the threats of interception, exploitation, and both intentional and unintentional interference.

2. Controls shall be in place to prevent replay of voice communications.

2.4.2 Encryption

The purpose of the encryption policy is to protect information being transmitted among communications components or devices by cryptographic means. The encryption policy is as follows:

1. Cryptographic components shall be used to ensure secure communications over the LMR system.

2. End-to-end encryption shall be implemented to ensure secure communications.

3. Encryption devices shall be physically secured when unattended or not in use.

4. Encryption algorithms shall be as defined for the Federal Information Processing Standards (FIPS) Publication 140-1 Security Requirements for Cryptographic Modules.

5. The system shall support over-the-air rekeying of encryption devices.
2.4.3 Key Management

The key management policy governs procedures for generating, storing, protecting, transferring, loading, using, and destroying cryptographic keying material (i.e., paper tapes, electronic keys, punch cards, and key codes). The key management custodian ensures that all keying material is protected from deliberate or inadvertent disclosure, theft, modification, or destruction. The key management policy is as follows:

1. Public keys shall be protected against unauthorized modification and substitution.
2. Procedures shall be in place that ensure proper generation, handling, disposal, and destruction of outdated keying material.
3. Proper management controls shall be in place for trunked keys.
4. Procedures shall be in place to safeguard all cryptographic material.

2.4.4 Firewall

The main function of a firewall is to centralize access control. The firewall policy governs procedures for protecting an organization’s network and its resources from unauthorized access and denial of service. The firewall policy is as follows:

1. A firewall shall be configured to deny all services not expressly permitted.
2. A firewall shall provide detailed audit logs of all sessions so that these logs can be reviewed for any anomalies.
3. A firewall shall be physically secured, and server configuration and management shall be performed physically at the server.
4. A firewall shall not support Internet Protocol (IP) routing or forwarding.
5. A firewall shall be configured to rewrite mail address headers to conceal information regarding the internal network.

2.5 Radio Security

The radio security policy ensures that radio communications will be available to public safety personnel at all times. The radio security policy is as follows:

1. Authentication procedures shall be established to ensure the authenticity of radio transmissions.
2. Authentication controls shall be established to ensure that only authorized radios are used for communications.
3. Radio systems shall recognize the failure of any repeaters and adjust accordingly to prevent interruption of communications.

4. The agency shall have 24-hour, two-way radio capability to provide continuous communications between the officers on duty and the communications center.

5. Radio management controls shall be in place throughout the radio life cycle (e.g., inventory control, lost and stolen radio controls, and disposal or destruction of unused radios).

2.6 Mobile Data Terminal/Mobile Computer Terminal Security

The MDT/MCT security policy ensures that users conducting transactions via MDT/MCTs are properly authenticated and have authorization to use the system. The MDT/MCT security policy is as follows:

1. Authentication controls and/or procedures shall be set up between the network and MDT/MCTs to prevent unauthorized transactions.

2. MDT/MCT management controls shall be in place throughout the terminal life cycle (e.g., inventory control, lost and stolen terminal controls and disposal or destruction of unused terminals)

3. Sensitive data shall be cleared from MDT/MCTs before the terminals are released for disposal or destruction.
APPENDIX A—REFERENCES

Commission on Accreditation for Law Enforcement Agencies, *Chapter 81 Communications Standards*, April 1994

Department of Justice, *Federal Bureau of Investigation Automated Data Processing Telecommunications Security Policy*, undated


Land Mobile Radio Security Planning Template, July 1999


Telecommunications Industry Alliance/Electronics Industry Association, Telecommunications Systems Bulletins (TIA/EIA TSB):

- TIA/EIA TSB 102-A *System and Standards Definition*, November 1995

Trans European Trunked Radio (TETRA) System Security Standards 02.22 *Security Objectives and Requirements*, October 18, 1993
APPENDIX B—GLOSSARY

Access Control

A technique used to define or restrict the rights or capabilities of individuals or application programs to communicate with other individuals or application programs or to obtain data from, or place data onto, a storage device.

Audit Trail

A chronological record of system activities that is sufficient to reconstruct and review the sequence of events surrounding or leading up to all transactions and actions performed on or by the system.

Authentication

The process of verifying the identity of a user, terminal, or application program to prevent fraud, abuse, and misuse of services.

Automated Information System

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

Availability

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

Communication Deception

Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications.

Communications Security

Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security and physical security of COMSEC material.

Computer Room

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

Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information.

Computer Security

Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware and information being processed, stored, and communicated.

Confidentiality

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

Configuration Management

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

Contingency Plan

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

Cryptanalysis

Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.

Cryptography

Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Cryptographic

Pertaining to, or concerned with cryptography.

Cryptosecurity

Component of COMSEC resulting from the provision of technically sound cryptosystems and their proper use.
Encryption

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

Firewall

An electronic boundary that prevents unauthorized users from accessing certain files on a network; or, a computer used to maintain such a boundary.

Identification

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

Integrity

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

Jamming

The intentional transmission of radio signals that interfere with the reception of signals from another transmitter.

Key

A series of characters used by an encryption algorithm to transform plain text data into encrypted (cipher text) data and vice versa.

Key Management

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

Land Mobile Radio

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

Mobile Computer Terminal

A computer device located in a vehicle that provides access to remote database files and to communications with the dispatch office.
Mobile Data Terminal

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

Over-the-Air Rekeying (OTAR)

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

Password

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

Public Key

The key of a public key pair that is published widely.

Security Plan

A document that outlines a site’s plan for securing its system.

Transmission Security

The methods used to protect transmission from interception, exploitation, and jamming by means other than encryption.

Vulnerability

A weakness in a system’s design or procedure that could be exploited by a threat to gain unauthorized access to a system or degrade the system’s availability.
### APPENDIX C—ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIS</td>
<td>Automated Information System</td>
</tr>
<tr>
<td>EIA</td>
<td>Electronics Industry Association</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standards</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IS</td>
<td>Interim Standard</td>
</tr>
<tr>
<td>KMF</td>
<td>Key Management Facility</td>
</tr>
<tr>
<td>LMR</td>
<td>Land Mobile Radio</td>
</tr>
<tr>
<td>MCT</td>
<td>Mobile Computer Terminal</td>
</tr>
<tr>
<td>MDT</td>
<td>Mobile Data Terminal</td>
</tr>
<tr>
<td>NPRG</td>
<td>National Partnership for Reinventing Government</td>
</tr>
<tr>
<td>OTAR</td>
<td>Over-the-Air Rekeying</td>
</tr>
<tr>
<td>PCCIP</td>
<td>President’s Commission on Critical Infrastructure Protection</td>
</tr>
<tr>
<td>PDD</td>
<td>Presidential Decision Directive</td>
</tr>
<tr>
<td>PMO</td>
<td>Program Management Office</td>
</tr>
<tr>
<td>PSWN</td>
<td>Public Safety Wireless Network</td>
</tr>
<tr>
<td>TETRA</td>
<td>Trans European Trunked Radio</td>
</tr>
<tr>
<td>TIA/EIA</td>
<td>Telecommunication Industry Alliance/Electronics Industry Association</td>
</tr>
<tr>
<td>TSB</td>
<td>Telecommunications Systems Bulletins</td>
</tr>
</tbody>
</table>
APPENDIX J

RESPONSIBILITY FOR ASSIGNED PROPERTY
Appendix J – Responsibility for Assigned Property

The Contractor shall have custodial responsibility for all Airports Authority physical property issued to its control with an acquisition cost of $500.00 or more, during the contract term. Authority personal property, which includes computer equipment, furniture, fax and copier machines, etc., will be tracked by: (i) Airports Authority-issued bar codes; (ii) if no Airports Authority issued bar code, then by serial number assigned by the manufacturer; or (iii) if no bar code or a serial number, such as furniture, a unique identification number issued by Contractor personnel for tracking purposes. This number will be of a type and range approved by the COTR. A property inventory of all issued assets shall be conducted on the first and last day of the contract term to determine Contractor responsibility of Airports Authority property. The inventory listing shall include the description of the property, bar-code number (if assigned), serial number (or ID number), acquisition cost, acquisition date, manufacturer, location and user. If the acquisition cost and date for an issued asset cannot be provided to the Contractor by the Airports Authority, then the Contractor shall provide an estimated acquisition cost and date for the inventory listing, subject to the COTR's approval. The Airports Authority will provide all equipment and supplies necessary to provide and track property by bar-code. Unscheduled property inventories will be conducted by the Airports Authority during the contract term. The Contractor accepts the issued property in "as is condition." The property will be returned to the Airports Authority in the same condition as issued, reasonable wear and tear expected. The Contractor is not liable for the loss or damage of Airports Authority property, except when such loss or damage results from negligence by the Contractor. The Contractor's responsibility stated herein is solely for the purpose of tracking Airports Authority physical property that is issued to the Contractor and that is used exclusively by the Contractor in the performance of its contract scope.
APPENDIX K

SMARTPHONE WAIVER FORM
SmartPhone Waiver Form

All Authority users requesting corporate email access through their personal SmartPhone using Microsoft Direct Push (Mobile Active Sync) must review and acknowledge the conditions outlined in this Waiver. Once completed and signed by the end user, the form should be forwarded to the IT Help Desk for processing. All requests for Direct Push will be reviewed and approved by the Information Systems (MA-610) Manager.

Conditions:

• Security:
  o Prior to accessing Authority mail via Direct Push, all SmartPhones (corporate and personal) are required to receive and accept a security policy sent from the Authority’s exchange server.
    ▪ This policy will implement and enforce a local security policy on the SmartPhone which will require a four digit pin to be set up on the local device.
    ▪ This policy will enable the “auto-lock” feature in the event the phone is unused for a period of time (the established pin is required to unlock).
    ▪ This policy will enable the Authority, at its discretion, to remotely manage and/or wipe the device in the event of loss or compromise.
      This reset will return the device to its factory default.
    ▪ The Authority will not be held responsible for loss of personal data or applications in the event of MA-610 using the remote wipe utility.

Note: In event your SmartPhone is lost or stolen, please contact the IT Help Desk as soon as possible. Action will be performed to remotely reset your Smartphone back to factory settings to prevent unauthorized access.

• Service and Support:
  o End user support provided for the IT Help Desk is limited:
    ▪ A configuration reference guide will be hosted and maintained through Livelink.
    ▪ Limited configuration support will be provided via telephone support.
    ▪ No carrier related support will be provided by the Help Desk (including coverage, service problems, plan selection, and etc.).
    ▪ No Hardware support will be provided for SmartPhone devices. Users will need to contact their wireless carrier for support.

  o Service Interruptions:
    ▪ Periodic maintenance and other conditions may result in temporary loss of Direct Push service. The Authority makes no claim to reliability of the service and the end user acknowledges as such.
    ▪ In the event of an interruption of service, a notification will be distributed by the IT Help Desk.
- The end user is solely responsible for the selection and purchase of all SmartPhone devices and data service plans.
- The device selected must support **Microsoft Direct Push (Active Sync)**.
- The device should have a data plan associated with it.
- We recommend unlimited data plan
- The costs incurred associated with the SmartPhone service and associated data plan is the responsibility of the end user. The Authority will NOT reimburse users for expenses associated with these services.

**Acknowledgement:**

I, _____________________________, have read the conditions outlined in this form and agree to be bound by them. Furthermore, I agree to not hold the Authority responsible for any costs associated with my personal SmartPhone hardware, service, or data plan. Finally, I request that the Direct Push service be activated for use on my personal SmartPhone and acknowledge that the mandatory security policy will be imposed on my SmartPhone device and that my device may be reset to its factory default state in the event of compromise, loss or upon termination of employment with the Authority.

SmartPhone Number: ________________________________

Make/Model of the Phone: ________________________________

Carrier Info: ________________________________

_________________________________________  ________________________
Requestor’s Name       Date

_________________________________________  ________________________
Approval (MA-610 Manager)      Date
APPENDIX L

INTEROPERABILITY WEB EXHIBIT
APPENDIX M

CALL ORDER FORM
## CONTRACT SERVICES CALL ORDER

**Prepared:** ____________________________  **Date Prepared:** ____________________________

**Type of Work:** ____________________________  **Requested By:** ____________________________

**Contractor:** ____________________________  **Contract #:** ____________________________

**Address:** ____________________________  **Contractor POC:** ____________________________

  **Office Telephone:** ____________________________  **Emergency Phone:** ____________________________

**Other Data:** ____________________________  **Contractor Fax:** ____________________________

**Location (Name, [Account Code]) and Description of Work**

<table>
<thead>
<tr>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Work Estimates

**Estimate Date:** ____________________________  **Site Vist Date:** ____________________________

**MWAA Estimator:** ____________________________  **Contractor Estimator:** ____________________________

**Work Item(s):** ____________________________  **QTY/UM:** ____________________________

<table>
<thead>
<tr>
<th>Work Item</th>
<th>QTY/UM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Estimated Cost:** ____________________________  **Notes:** ____________________________

### APPROVALS / ACCEPTANCE OF TASK

**NOTE:** By signing this Call Order, the Contractor acknowledges that he/she will only perform the work described herein after this Call Order is approved in writing by the COTR. Furthermore, the cost to the Authority for this work shall not exceed the “Estimated Cost” noted above.

**Call Order #**

<table>
<thead>
<tr>
<th>Call Order</th>
<th>MA-110 or 210:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Date:_________ Date Issued:_________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Call Order</th>
<th>COTR:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Date:_________ Date Completed:_________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Call Order</th>
<th>Inspector:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Date:_________ Date Invoiced Rev’d:_________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Call Order</th>
<th>Contractor:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Date:_________ Invoice Amount:_________</td>
</tr>
</tbody>
</table>

**Remarks:** ____________________________