Metro Emergency Radio Management Committee (MRAM)

800 MHz Radio Systems Standard Operating Procedures

Table of Contents

STANDARD OPERATING PROCEDURES

Adoption/Approval Document

METROPOLITAN GOVERNMENT OF NASHVILLE & DAVIDSON COUNTY
DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES
PO BOX 196300
NASHVILLE, TENNESSEE 37219-6300

The Chief Information Officer (CIO), under the direction of the Metro Emergency Radio Management Committee has approved and adopted the attached **STANDARD OPERATING PROCEDURES (SOPs) FOR THE METRO NASHVILLE/NES - 800MHz RADIO SYSTEM** on this 21st day of September , 2017. This SOP shall remain in effect until revised, replaced, or withdrawn under this authority.

Authorized Signatures:

(Printed Name) Signature	Title/Agency	Date
KEITH DURBIN	CIO / ITS	11/16/17
Margaret H Keck	Assistant IT Director / ITS	11/16/17

NIMS COMPLIANCE REVIEW

Metro Nashville and Davidson County has adopted the National Incident Management System (NIMS) as the framework for management of all emergency incidents within its jurisdiction. Establishing standardized operating guidelines, procedures, and protocols for utilization of interoperability resources is directly aligned with the objectives and initiatives contained in the National Emergency Communications Plan (NECP), as well as the Communications and Information Management Component of NIMS.

NIMS elements addressed by or embedded in this SOP document include:

- Usage of common terminology and nomenclature
- A mechanism for establishing a common operating picture
- Common technology platform for interoperability
- Potential solution for strategic, tactical, and support communications
- Communication of incident information
- Radio usage procedures
- Training and exercises

Authorized signature(s) below confirm that this SOP document has been reviewed by Metro's Office of Emergency Management (OEM) for compliance with the National Incident Management System.

(Printed Name) Signature	Title/Agency	Date
Heidi Mariscal, Heidi Mariscal	Planning, OEM	12-19-17
Joseph M. Clinard III	Radio Communications Manager	12/19/2017

MRAM SOP REVISION RECORD

CHANGE#	DATE	SECTION	DESCRIPTION	APPROVED BY
001	03/21/2019	5.17 Encryption	Use of encryption will be determined by the talkgroup owner	
002	03/21/2019	5.18	Changed to specify all Metro agencies and departments are subject to this section, and that all installations must meet building and fire codes	

1.0 INTRODUCTION

The MRAM SOP provides NIMS compliant procedures that are applicable to multi-agency, multi-discipline, all-hazard responses throughout Metro Nashville (Metro). This SOP insures consistent protocols and formalizes the operation and usage of the 800MHz Radio System (System). This SOP will be utilized by Metro's emergency response and support personnel, communications operational and technical personnel, state/local/Federal government representatives, non-governmental organizations (NGOs), and other system users as authorized by MRAM.

All System users are expected to comply with this SOP.

2.0 PURPOSE

The System is a mixed mode radio communications system designed to meet the needs of Metro's law enforcement, emergency management, fire, emergency medical, public health, correctional, transportation and public works responders and any others who are supporting emergencies, events and disaster response across the State.

This SOP addresses procedural and operational aspects of the System to include:

1. Operational guidelines
2. Technology specifications and requirements
3. Usage guidelines
4. Training and exercises
5. Maintenance and repair

2.1 Governance

The Metro Emergency Radio Management Committee (MRAM) was created by the Mayor's executive order to purchase, construct, and operate an 800 MHZ trunked radio system to improve emergency dispatch and response throughout Davidson County.

The order creating MRAM charges the committee with managing the access and operation of the 800 MHZ trunked radio system, and also specified the composition of the committee.

MRAM is governed by a committee of twelve voting members, specified in the order, and non-voting representatives of other user agencies composed of both public safety and public service agency officials.

The committee reviews and approves system access requests, and refers them to the Metro Legal Department for development of Interlocal Governmental Agreements and/or a Memorandum of Understanding prior to official approval by the Metro Council.

2.2 What is the Metro Emergency Radio Management Committee (MRAM)

MRAM was originally created by Mayor Phil Bredesen's Executive Order No. 99-06, and was continued by Mayor Bill Purcell' s Executive Order No. 18, Mayor Karl Dean's Executive Order No. 29, and Mayor Megan Barry's Executive Order No. 19, a copy of which is found in Appendix 1.

The Committee consists of representatives from every user department and agency, and is chaired by the Chief Information Officer (CIO) or his/her designee. Voting privileges are reserved for the following agencies only:

- Metro Nashville Police Department (MNPD), 2 votes

- Metro Fire Department (MFD), 2 votes
- Information Technology Services (ITS), 2 votes
- Nashville Electric Service(NES), 2 votes
- Department of Emergency Communications (ECC), 2 votes
- Office of Emergency Management (OEM), 1 vote
- Department of General Services (DGS), 1 vote
- Davidson County Sheriff's Office (DCSO), 1 vote
- Department of Public Works (PW), 1 vote
- Metro Parks and Recreation Department (Metro Parks), 1 vote
- Metro Water Services (MWS), 1 vote
- Metro Purchasing Agent, 1 vote

The mission of the Committee is as follows:

- Develop and implement guidelines for the allocation of effective and efficient use of the System, including the loading and development for all users.
- Review and disseminate the annual recommendations provided by the Director of Finance that relate to a fair and proportionate rate structure by which to assess each user for the recovery of maintenance and operating costs of the System.
- Provide long-range planning for the continued operation of the System.
- Consider, review, make recommendations for, and resolve all requests for system access or connection.

The committee meets on the third Thursday of January, March, May, July, September, and November at 9:00am.

2.3 What is the Technical Committee

The Technical Committee is a sub-committee of MRAM that is charged with the oversight and review of all technical aspects of the configuration and operation of the System. The Technical Committee receives direction from the MRAM Committee and provides observations and makes recommendations on projects, procedures, upgrades, and system access.

Individual committee representatives are selected by each department, and should have technical knowledge of radio systems and operations. The Technical Committee meets every month on the second Thursday at 11:00am.

2.4 What is the 800MHz Radio System?

The 800MHz Radio System (System) is an advanced analog and digital radio communications system built to the Association of Public-Safety Communications Officials (APCO) Project 25 (P25) digital radio standards, with a legacy Motorola SmartNet component. The System utilizes radio frequencies in the 800 MHz and microwave radio spectrum under the rules and regulations of the Federal Communications Commission (FCC).

Motorola Solutions, Inc. constructed the system infrastructure.

- Construction of the SmartZone system was completed in 2000. Two separate systems of 18 channels were built, designated the 'A System, and 'B System'. The 'A System' was dedicated to public-safety agency operations, and the 'B System' was dedicated to public service entities and other non-public safety users.
- The 'A System' was upgraded beginning in 2011 to the APCO P25 interoperability standard for public safety communications systems, and was renamed the 'P25 System.
- Additional migration of channels and users from the 'B System' to the 'P25 System began in 2016, with completion planned for 2020.

The System consists of the following major components:

1. Radio communications sites (towers, equipment shelters, generators & site security)
2. Radio spectrum in the VHF, UHF, and 800 MHz frequency bands and microwave radio frequency spectrum
3. Radio Tower sites located diversely across the county
4. Microwave radio links between the radio sites and the public safety communications center
5. Subscriber Units – mobile, hand held (portable) radios and control stations
6. Service and maintenance facilities

The System is designed to provide 90% mobile radio reliability throughout the Nashville Electric Service (NES) service area, 95% mobile radio reliability within the Davidson county borders, and 95% outdoor portable radio reliability within the Briley Parkway / Thompson Lane / Woodmont Blvd. / White Bridge Road loop.

2.5 Eligible Users

The primary purpose for the System is to support Metro's public safety responders and NES. Any Metro Nashville Government Department or Agency or Nashville Electric Service Department is eligible. Local, State, and Federal government agencies may be eligible, if system capacity or coverage is not an issue.

2.6 Acceptable Usage

All System users are expected to follow these acceptable use policies.

The System is to be used for day-to-day operations, emergency response calls, incidents, missions and disasters. The System may also be utilized for planned events, training and exercises, if there is sufficient channel capacity and the planned activity has been coordinated and approved prior to its start date.

2.7 Radio Discipline

Purpose or Objective
To define the policy for the acceptable usage of the System.

Operational Context
This policy is to act as clearly defined discipline for agencies/entities to follow when using radios on the System. Each agency/entity is responsible for ensuring their users adhere to proper radio discipline.

Misuse of the system will be reported to the Metro CIO to handle directly with the agency/entity department head or his/her designee. The reporting parties contact information should be provided in the notification. No profanity, playing music, personal conversations or activities not directly related to public safety will be permitted on the system.

All agencies/entities are expected to utilize these resources sparingly. Users should keep radio conversations as concise and short as possible.

All agencies/entities utilizing the System must abide by all FCC regulations as stated in Title 47 Part 90 Land Mobile Communications.

3.0 SCOPE

This SOP applies to the operational, technical and usage aspects of the System. It is therefore applicable to any user of the system, and applies to government agencies at the municipal, county, state, and federal levels, as well as applicable NGOs.

3.1 SOP Approval

This System SOP and subsequent revisions require approval of the MRAM Committee after review by the CIO.

3.2 SOP Change Process

Annual Review Requirement

The SOP will be reviewed on an annual basis to assess the need for updates or revisions. The CIO or their designee (e.g., MRAM User Group) will be assigned the task of reviewing the SOPs, identifying applicable updates, and submitting a draft of the revised SOP for approval.

Operational Context

MRAM is charged with setting standards and determining protocols and procedures for optimal operations between and among the users of the System.

Reviewers

Under the direction of the MRAM Technical Committee, this SOP will be reviewed annually by an appointed task team to determine if changes are warranted. Upon completion of the review, the task team will present to the MRAM Committee:

- Written report of all findings
- Recommended changes

Submitting Change Requests

Requests to delete, add, and/or change adopted standards, policies and/or procedures may be submitted in writing to the MRAM Committee at any time. If the requested change is time critical, the MRAM Committee may direct a request for immediate consideration to the MRAM Technical Committee.

Change Request Contents

A written request for any change to the SOP submitted to the MRAM Committee shall include:

- A full description of the deletion, addition, or change including section and sub-section references
- The reason for the change (including the potential consequences if the request is not approved)
- A preliminary assessment of impact on other system users and an estimate of associated costs, if any.

At the discretion of MRAM, the request can be forwarded to the Technical Committee for review, analysis and/or recommendation, or MRAM may take immediate action.

MRAM may direct its Technical Committee to conduct an assessment to address:

- Technical impact to current and future system performance including which system or subsystems will be or may be affected;
- Operational impact to current and future system performance including effects on system capacity and determination of those systems or subsystems that will be or may be affected;
- Degree of conformance with MRAM plans and standards;
- Cost impact to current participants and;
- Potential alternatives.

The Technical Committee shall forward the completed assessment to the MRAM Committee along with recommendations including strategies to mitigate negative impacts, if appropriate.

The MRAM Committee shall notify all agencies of all requests along with potential impact and invite their comments.

The MRAM Committee will approve, deny, or modify the requested SOP change and will inform all parties of their decision.

If approved, MRAM will incorporate the applicable SOP modifications and inform system users.

Management of Change Process

The MRAM Chairperson will manage this process.

4.0 RADIO SYSTEM MANAGEMENT

4.1 Radio System Architecture

The System is an advanced digital radio communications system built to the Association of Public-Safety Communications Officials (APCO) Project 25 (P25) digital radio standards, with a legacy Motorola SmartNet component. The P25 System is a standards based system, and different vendor subscriber radios will be able to access and use it. Due to manufacturer differences outside of the defined P25 standard, not all manufacturer radio features may work with the system. Some radios may interact differently with the existing infrastructure and can potentially exhibit undesirable operational characteristics.

As a result, the following procedures must be followed:

- All manufacturers' radios must be tested and approved by Metro Radio Communications prior to being used on the system.
- A listing of tested and approved radio models will be maintained by the Radio Communications Subscriber Services office.

Operational Context

The system is dedicated primarily to public safety agencies, the agencies that support public safety, and public utility and service agencies.

Protocol / Standard

The System utilizes the APCO Project 25 Phase 1digital radio standard, for the voice and control channels. The microwave radio is a digital system that adheres to Telecommunications Industry Association (TIA) / Electronic Industry Alliance (EIA) industry standards.

4.2 Radio System Management

The ITS Radio Communications Division is responsible for the day-to-day management, operation and oversight of the System and for the maintenance of this SOP. System administration is the responsibility of the Radio Communications Manager. Complete details on system Governance are contained in a separate governance document.

The Radio Communications staff makes decisions on issues related to the day-to-day operation of the System and addresses urgent or emergency system operational, maintenance, or repair decisions.

An urgent or emergency situation is one where immediate decision authority is needed to allow the system as a whole, or any of the subsystem components, to continue supporting normal wide-area voice communications services. It is recognized that Radio Communication staff may have to obtain authorizations from the MRAM Committee to make longer-term or non-emergency capital or repair expenditure decisions.

The ITS Radio Communications staff is responsible for the day-to-day management, operation and oversight of the system. While their specific duties are not detailed in this document, their general duties include:

- Monitoring the systems and components for normal operations
- Diagnosing system performance, problems, and developing corrective action recommendations
- Dispatching appropriate repair services in the event of a malfunction of system equipment
- Managing the database elements, including subscriber IDs, talkgroup IDs, and the various parameters that relate to their effective operation
- Working with all agencies and their technical staff to diagnose and resolve problems that involve radio operations, maintenance or repair of the equipment
- Serving as the point of contact (POC) with equipment manufacturers for issues related to the radio systems
- Providing timely information to system users on issues that arise, or repair/maintenance issues related to system equipment that would affect normal radio operations
- Monitoring the performance of the entire network for normal operations
- Monitoring system databases for normal operations and conducting regular database backups
- Monitoring channel capacity and system loading level averages to ensure that they remain at or below fifty percent, that system busies do not exceed one percent, and wait times do not exceed two seconds during normal daily operations

Due to the complexity and distributed administration and maintenance of the system, problems can typically occur when changes are made to hardware or software. In order to keep all representatives informed of any updates, notifications are sent to all primary and alternate user agency MRAM representatives when the following actions occur:

- Planned maintenance work is being performed on the systems that will impact performance or system operations
- Equipment malfunctions or failures that affect system performance or operation
- Configuration changes in equipment or software by any user agency that may impact operations of any other agency

The Technical Committee meetings are held each month to review operations of the systems and to share ideas or issues that have arisen and may be of interest to user agencies.

4.2.1 System Security

Any computer, netbook, tablet, or data storage device that will be connected to the system for maintenance, programming, updates or other needed functions must be virus and malware free. Any such device must also be supported and maintained by the technician's, agency's, or vendor's Information Technology department or service provider to ensure the most current device security software and virus protection is in place.

A 'Group Policy' shall be implemented on the System to prevent the use of external USB ports on all dispatch consoles.

At no time will a personally owned device of any kind be allowed to be connected to the System. Any such action will result in the immediate revocation of access privileges for the offender and/or agency.

Violations of system security policy or procedures may jeopardize the system and result in the loss of a technician's, agency's, or vendor's privileges to access the system.

4.2.2 System Loading

The ITS Radio Communications staff is responsible for monitoring the System's channel capacity and traffic loading levels to ensure that during normal daily operations:

- The average maximum system load is at or below fifty percent
- That system busies do not exceed one percent, and
- Wait times do not exceed two seconds

When the system load consistently approaches or exceeds any of these limits, Radio Communications staff shall immediately notify MRAM of the situation and begin planning for additional capacity if necessary.

4.3 Network Management

Purpose or Objective

Defines the responsibilities for network management.

Technical Background

The System is comprised of, but not limited to, channel banks, hubs, switches, routers, servers, local area networks, and wide area network links connecting sites together. The

network sites are interconnected by usage of microwave radio equipment, fiber, or telecom T1 circuits. The radio network is monitored with network management tools provided by the equipment manufacturers.

The radio system architecture is primarily constructed around the APCO Project 25 standard. The microwave system is composed of industry standard equipment, which also provides flexibility and a large variety of management and diagnostic tools.

The system network is complex and unusual problems may be difficult to identify and resolve. System documentation shall be kept up to date or it will lose its value in supporting the system network.

The System is protected from all other agency data networks to protect the security and functionality of the system. If there is a connection to another data network, it is through an appropriately designed and manufacturer approved and supported firewall.

Operational Context

The components of the System are considered as "owned" by ITS, which is responsible for the maintenance of the sites and equipment. Agreements between ITS and maintenance contractors are at the discretion of ITS.

The backbone of the system is structured on an integrated network. Any infrastructure hardware and software upgrades or changes that may impact the system require reasonable discussion, approval, and oversight by ITS Radio Communications, and the MRAM Committee.

All maintenance work being scheduled that may affect system performance is preceded by reasonable and appropriate notification to the user agencies.

The configurations for each of the components of the system are documented primarily for the purpose of maintenance but also affect future planning. The manufacturer provides the original 'as built' documentation.

The other defined standards for maintenance, documentation, notification, changes, security, and training also pertain to the network portion of the systems.

Procedure

The methods for performing detailed system operations are defined in the technical resource manuals and training documentation for the systems. The technical resource manuals are classified as 'Restricted Information' in accordance with the ITS Information Classification Policy and are not available to the general public except by formal written request approved by MRAM, the CIO, and Metro Legal.

4.4 Advanced System Keys

Purpose or Objective

To outline the procedures for the production, issuance, and usage of both the Software and Advanced System Keys (ASK) for the System.

Technical Background

A system key allows for the programming of a radio for use on the system and is used to maintain system security. The system key keeps unauthorized units from gaining access to the system. Most radio equipment manufacturers provide a unique software based system key unique to each trunked radio system. The system key is required for a radio (subscriber unit) to be programmed so that the radio can be recognized by the system and the user can access the system. Without the proper system key, a radio can neither access nor communicate on the system.

Operational Context

The Radio Communications Division of ITS will maintain and safeguard all Master ASKs, regardless of the manufacturer and is responsible for the production and issuing of all secondary keys to authorized users. Manufacturers' radios that do not require a system key will not be approved for operation on the system.

An agency using subscriber radios other than the system manufacturer, Motorola, must acquire and provide to the Radio Communications Division the manufacturer's Master ASK for the 800MHz System and all necessary software and key hardware to program secondary keys as needed.

Each secondary ASK will be programmed for only the subscriber ID and talk group ranges approved for that agency. No secondary ASKs will be produced with an expiration date to exceed one year. All secondary ASKs will be password protected.

Software system keys will not be used unless approved by the Radio Communications Manager.

Radios requiring a software system key will only be programmed by the Radio Communications Division staff, an authorized agency or authorized vendor. The safeguarding of these keys is paramount and should at all times be treated as restricted, public-safety sensitive information with access closely guarded.

Protocol

ASKs will be issued to and signed for by the lead agency for the local or state agency with authorized access. These key holders may sign out their key within their agency or to authorized secondary vendors to have their radios programmed.

Each key holder should maintain a log of who the ASK was issued to, agency or company, the date issued, the date returned, a signature and a phone number. All copies of the system keys must be kept in secure areas within the control of the key holder and only shared with those requiring knowledge of it for operational purposes.

The system key is not available to anyone outside of Metro or authorized users, except by formal written request to the MRAM Committee and are not to be released to any personnel not having a legitimate and appropriate need.

Procedure

Once a radio is programmed, the user agency will need to notify Metro Radio Communications staff and provide the following information:

- Agency
- Radio User information (position or name)
- Radio Serial Number
- Model Number
- Flash Code
- Radio ID Number (decimal & HEX)
- Radio Alias
- Date Issued

No radio will be activated in the system until all requested information is received by Metro Radio Communications. Radio Communications staff will activate radios within two working days of receipt of above information.

During times of emergencies or disaster, additional subscriber units may need to be activated quickly. In this event the Radio Communications Manager may approve the additional subscriber units for immediate programming and activation. These units will be deactivated after the event is over unless prior arrangements are made.

Management

The Radio Communications Manager is responsible for maintaining the security of and access to the system keys.

4.5 Database Management

Purpose or Objective

Defines the aspects and assignment of responsibilities for managing the System's databases.

Technical Background

The management of the system and subsystem databases is assigned to staff with responsibility for the various aspects of the system operations.

The databases contain objects for the system and subsystems defining the operational characteristics of:

- Subscriber Radios
- Radio Users
- Talkgroups
- Profiles for Radio Users and Talkgroups

- Storm Plans
- System portion of the fleet map programming
- System and Subsystem equipment operational parameters
- Security Group structures
- Login User accounts and privileges

The databases contain the operational personality of the entire system. Because of this critical function, the data must be properly managed for system functionality and archived regularly in case of data loss or corruption.

The databases do not contain equipment programming parameters for such things as routers, switches, hubs, channel banks, etc. Nor do the databases contain the software load information of servers and client computers.

Operational Context

The system databases are partitioned to facilitate the distributed management of the data contained in them. Radio Communications staff shall manage the portions of listed data in this section.

Radio Communications is responsible for maintaining and archiving copies of all radio codeplug data and system databases.

Database backups are made once per week and are stored “off-site” on a backed-up server in the event of a disaster.

Database restoration will be performed by trained technical staff and only in the event of system software reloading and version changes, system database corruption, or as defined in the Disaster Recovery Plan.

Database restoration is performed when a non-critical condition exists and if approved by Metro Radio Communications.

The Radio Communications technical staff notifies agencies of any database issues that may adversely impact their normal operations.

Protocol

To gain access to the system database, a request from the individual’s home agency along with proof of training must be submitted to the Radio Communications Manager. A sample access form is found in Appendix 4, however, an official form should be requested from the Radio Communications Manager. Adherence to the System Security policies and protocols are critical to the safe operation of the system.

Procedure

The methods for performing the database operations are defined in the manufacturer’s technical resource manuals. The technical resource manuals are classified as ‘Restricted

Information' and are not available to the general public except by formal written request to Metro Radio Communications.

The procedure for this standard is at the discretion of Metro Radio Communications.

Management
The Radio Communications Field Services office is responsible for managing the data attributes and is responsible for backing up the system databases.

4.6 Radio Issuance, Assignment, and Replacement

Purpose or Objective
Establishes the policy to ensure all radios activated on the system are properly managed, assigned, and accounted for, and that replacement radio equipment is readily available to Metro public-safety responders when needed.

Technical Background
Radio Communications manages the radio equipment inventory and is responsible for issuing replacement radios as necessary.

The radio system's controller provides individual access to the radio system for each assigned radio.

An individual radio user may have more than one radio assigned to them depending on their job function.

In order to avoid potential dispatcher and radio user confusion, and delays in requests for assistance, individual agencies are seriously discouraged from holding 'spare' radios and using generic radio aliases.

Operational Context
During normal working hours, individual radio users must obtain issuance, repair, and replacement of Metro owned mobile and portable radio equipment from the Radio Communications Office at the Metro Southeast facility.

Replacement of subscriber radios is only provided at the MSE location during normal working hours.

Radio Communications shall not issue 'spare' or 'extra' radios to any agency without prior approval from the Director of ITS and MRAM.

Protocol/ Standard
A lost or stolen radio cannot be replaced until a police report is submitted as described in Section 4.7.

Radio Communications will maintain a record of all current and past radio assignments on the system, which will also include radio assignments for the previous 12 months. This record will be kept on a secure server for a minimum of one year.

Management
Radio Communications is responsible for managing this policy.

4.7 Lost or Stolen Radio Notifications

Purpose or Objective
Establishes the policy to ensure the System's operational integrity and security by providing users with a procedure for reacting to incidents of missing, lost or stolen radio units.

Each agency shall develop internal guidelines for dealing with incidents of lost, stolen or missing radio equipment.

Technical Background
The radio system's controller provides individual access to the radio system for each assigned radio. The controller provides the ability to regroup or lock a specific radio to a specific talkgroup or to disable the radio altogether with the 'Inhibit' feature.

The target radio must be turned on and affiliated with the radio system for the actions to be processed. If the target radio is not active, the requested action can be put into the passive mode. When the target radio does attempt to affiliate with the radio system, the pending action is initiated.

Operational Context
All agencies are required to make immediate notification to Radio Communications upon receiving information, notification, or recognition that an assigned radio is misplaced, lost, or stolen. Delay in providing notification could result in unauthorized persons causing interference and/or receiving confidential information.

Protocol/ Standard
Radio Communications shall be immediately notified of the situation by a phone call and a Radio Equipment Damage/Loss Form found in Appendix 9.5 must be submitted.

A damaged, lost, or stolen radio cannot be replaced until a Radio Equipment Damage/Loss Report is submitted to Radio Communications.

For any lost or stolen equipment, the agency or user is required to obtain and submit a police report to Radio Communications no later than 5 working days after the loss.

Lost and stolen radio information will be passed on to user agencies and local radio shops in case the radio is located or turned in.

Radio Communications will invoice the agency for the replacement cost of the radio if owned by ITS.

Management
Radio Communications is responsible for managing this policy.

4.8 System Management Access

Purpose or Objective
Defines the types and areas of individual access to the management functions of the system.

Technical Background
Every login user of the system has a minimum of one login account and possibly more if multiple levels of access rights are needed for different purposes, such as administrative or general use. Every account can be individually set with the security and application rights needed to meet the needs of each user. All user account IDs shall be unique as the system's databases do not permit the use of duplicate IDs. The user login aliases are limited to a specific length.

Operational Context
Personnel who log into the systems to use management applications and support tools are referred to as "Login Users". These are technical support staff such as the system manager, administrators, technical support staff etc. This is different than "Radio User" as referred to in other standards. Every user's login ID on the system is unique. Every login user of the system has a user ID that is only for that specific agency's or individual's use. Based on the types of access required an individual may need more than one login ID.

The types of access fall into the following areas:

- System Management
- Infrastructure Maintenance
- Subscriber Administration
- Dispatch Management
- Asset Management

The areas of access are based on the physical locations of the equipment and individual need.

Access to System, Network, and Asset Management terminals will be limited to ITS Radio Communications and NES staff and approved vendors.

If an agency has need for a management terminal, and has justification, a request may be made in writing to the MRAM Committee.

An annual review of personnel with system access shall be performed to ensure that only the appropriate levels of access have been granted based on their currently assigned business needs.

Protocol

Each Login User account must be requested from and approved by the Radio Communications Manager. The account will be assigned a login name and access level based on the requirements of the request. Access will be immediately rescinded for any unauthorized actions or change of employment status.

Management

The Radio Communications Manager is responsible for the creation of administrative accounts, designating the areas of access allowed for each account, and the annual review of access granted.

4.9 Requesting System Access

Purpose or Objective

To establish the procedure for an eligible agency to apply to participate on the 800 MHz System.

Technical Background

Agencies requesting participation shall be prepared to purchase, negotiate a lease agreement, or already own 800 MHz digital trunking radios approved by MRAM. In addition, participation could require the purchase and installation of additional equipment, features, and/or options in order to be compatible with Metro's system.
Certain radio makes and models are not able to access the Metro system. MRC shall be consulted to ensure the specified equipment can operate correctly and is approved for the system prior to submitting a request for access.

Because of the limited number of available failsoft channels, outside agencies may not be granted a failsoft channel assignment, and will receive a lower priority for all talkgroup assignments, however interoperability access is not affected by this policy.

Operational Context

All agencies eligible to join the 800 MHz System shall do so in accordance with, and meet the requirements of, this manual. Operational plans shall be consistent with established standards.

Each agency controls outside users access to the agency's individual talkgroups. MRC will not give access to any talkgroup without first having the written approval of the appropriate agency.

Recommended Protocol/ Standard

Requests for access to the 800 MHz radio system are submitted in writing to MRC, who will forward the request to all required parties for approval. If the requestor desires access to specific agency talkgroups other than their own, then the request shall include a full explanation of the expected use of those talkgroups requested, and a justification of the same.

Recommended Procedure

The access request form should be obtained from MRC, completed by the requesting agency's representative, and returned to MRC for processing.

The request shall provide an outline of plans the requesting agency has for participation, and shall indicate the name and contact information for the person designated to lead the project.

The chair of MRAM or their designee shall forward copies of the request to the Technical Committee for review to ensure compliance and compatibility with MRAM's requirements. The Technical Committee shall then report its recommendations to the MRAM.

MRAM shall act on the request within a reasonable time period. MRAM can accept the request as submitted, accept the request with conditions or deny the request. If the request is initially denied, MRAM shall provide details on changes or additions to the plan that brings the plan into compliance with MRAM's requirements.

MRAM cannot deny the request if the design plan is compatible with MRAM's recommended changes or additions.

Management

MRAM is responsible for final approval of requests after an agency has approved or denied the request. MRAM will not grant access if denied by an agency.

4.10 Alias List Standards

Purpose or Objective

Establishes policy and procedures for maintaining the System's Alias database.

Technical Background

Login user, radio user and radio zone aliases are stored within system databases and are maintained by Radio Communications.

Having the Agency Alias table readily available to staff facilitates agency planning and assists agencies with reference information on identifying ownership of radio zones and users. Radio Communications staff keeps the Agency Alias table up-to-date and stored in a central location.

Operational Context
Radio users and zones are prefixed by an agency ownership acronym, as defined in the Naming Standards section of this manual. Depending on the agency name, the first characters are specified in the naming standard. Additional agency subdividing in the acronym table is optional.

Because assignments change over time, radio call numbers should not be used as an alias. It is suggested that individual radio aliases should reflect either the individual user (such as an employee number), or vehicle decal and position.

Procedure
Radio Communications manages the contents of the Agency Alias table.

Management
The Radio Communications staff is responsible for maintaining, archiving, updating and distributing the Agency Alias table.

4.11 Variances & Waivers

Purpose or Objective
Defines the process by which variances or waivers to these standards, protocols and procedures are granted to a requesting agency.

Operational Context
The MRAM Committee is charged with setting standards and determining protocols and procedures for optimal operations between and among the users of the System.

During times of disasters or emergencies, the Radio Communications Manager may approve a request if the variance or waiver is in the best interest of the system and those using the system. An example of a need for a variance or waiver would be loss of a radio tower during a disaster

Variance is defined as an allowed divergence from full adherence to an adopted standard, protocol or procedure.

Waiver is defined as a complete release from an adopted standard, protocol or procedure.

Variance/Waiver Request Protocol
Each request for variance or waiver from the adopted standards, protocols and/or procedures shall be made in writing to the Radio Communications Manager.

- The Radio Communications Manager will address short-term, incident-based, or time-critical variance requests that do not exceed 90 days in duration.
- Long-term (greater than 90 days in duration) or non-time-critical variance requests will be submitted to and addressed by MRAM.

Variance/Waiver Request Contents

A written request for a variance and/or waiver submitted to the Radio Communications Manager shall include:

- description of the desired variance or waiver including section and sub-section references
- reason for the variance or waiver (including the potential consequences if the request is not approved)
- preliminary assessment of impact to other system users, and an estimate of any associated costs to implement the request

At its discretion, the MRAM Committee may act on the request, but will generally forward requests to the Technical Committee for review, analysis and/or recommendation.

- The MRAM chair or their designee, in consultation with the requesting agency and Radio Communications staff, can approve a temporary variance or waiver until the official process is completed.

- Emergency deviations from the standards shall be communicated to all affected parties.

An assessment shall be conducted by the Technical Committee and shall address:

- technical impact to current and future system performance including which systems or subsystems are affected
- operational impact including capacity impact to current and future system performance
- the degree of conformance with MRAM policies and standards
- cost impact to current participants
- potential alternative solutions

The Radio Communications Manager shall forward the completed assessment to MRAM along with recommendations including ways to mitigate negative impact if appropriate.

MRAM shall advise all affected agencies of all requests, along with potential impact and invite comments.

MRAM shall approve, deny or modify the request and shall notify all affected parties of the decision. If approved or modified MRAM shall set forth operational and/or financial responsibility as appropriate and notify all affected parties.

Management

The Radio Communications Manager, acting on behalf of the Committee, shall manage this process.

4.12 Infrastructure Equipment Standards

Purpose or Objective

Sets the minimum technical and performance standards for infrastructure equipment operating on or interfacing to the System and establish a policy avoiding premature obsolescence of the same.

Technical Background

The 800MHz Radio System is an APCO P25 standards-based system constructed by Motorola Solutions, Inc. It consists of radio communications sites utilizing 800MHz radio spectrum. The Master Site is located at Metro's Emergency Communications Center. Microwave links between the Master Site and the radio sites utilize redundant methods in the construction of the system to provide for a public safety grade of service.

Vendors' equipment often utilizes different operating software and may interact differently with the existing infrastructure and can potentially exhibit undesirable operational characteristics.

It is also possible that new, untested radios, equipment and/or software can exhibit performance and functionality characteristics that are destructive to the performance, capacity and/or security of the System.

Operational Context

Participants desiring to connect or interface to the System any type of fixed equipment such as a radio or console products must first formally request and receive approval from MRAM. Prior to approval the system manufacturer must prove equipment compatibility. The approval must be vetted through the normal request process. All equipment must be installed in compliance with all rules, regulations and codes applicable to its operation and location, using industry accepted radio site installation and equipment grounding practices such as R56 or equivalent when possible, in effect at the time of installation.

Protocol

To ensure the reliability of the system, all infrastructure equipment directly interfaced to the System's core must maintain the same level of software revision.

Requests shall follow the normal approval process and must be submitted in writing to MRAM signed by the requesting agency director or department head.

Procedure

The request shall provide an outline of plans the requesting agency has developed for equipment integration. The written request shall indicate the name and contact information for the person designated to lead the project.

The chair of MRAM or their designee shall forward copies of the request to the Technical Committee for review.

If a technical use plan is already in place, the agency shall submit the plan to the Technical Committee for review to ensure compliance and compatibility with MRAM policy, standards, and procedures. If a technical use plan is not in place, Radio Communications staff shall assist the requesting agency in developing a plan. Costs associated with the development of a technical plan are borne by the requesting agency. When the plan is complete it is submitted to the Technical Committee, which shall review the plan for compliance and compatibility with MRAM's policies and procedures. The Technical Committee shall then report its recommendations to MRAM.

MRAM shall act on the request within a reasonable time period. MRAM can accept the request as submitted, accept the request with conditions or deny the request. If the request is initially denied, MRAM shall provide details on changes or additions to the plan that brings the plan into compliance with MRAM's standards.

Following making the design changes to bring the agency's plan into compliance with MRAM, the requesting agency must resubmit the request. MRAM should not deny the request if the design plan is 100% compatible with MRAM's recommended changes or additions.

Management
The Radio Communications staff is responsible for management of this procedure.

4.13 Subscriber Equipment Standards

Purpose or Objective
Sets the minimum technical and performance standards for subscriber radios operating on the System including:

(1) Establishing a policy avoiding premature obsolescence of subscriber radios and
(2) Establishing procedures for MRAM to measure, test, certify and publish a list of subscriber radios that are approved for use on the system.
(3) Ensuring that de-commissioned radio subscribers are properly de-programmed before disposal to prevent interference with public-safety communications

Technical Background
The System utilizes digital communication technology with the primary use being voice communications using the APCO P25 Phase 1 protocol with 9600-baud control channel and Motorola Astro Digital protocol with a 3600-baud control channel.

Subscriber radios from different vendors often utilize different operating software providing a variety of services, features, functionality and performance to the users. Many of these radios interact differently with the infrastructure and can potentially exhibit undesirable operational characteristics. An example of an undesirable operational characteristic is poor simulcast audio recovery that results in reduced geographic range, garbled audio, etc.

It is also possible that new untested radios and/or software can exhibit performance and/or functionality characteristics that are destructive to the overall performance, capacity and/or security of the System.

Decommissioned radios that are not properly deprogrammed could pose potential interference issues with public-safety communications.

Operational Context
System users require radios that meet operational needs and fall within budget constraints. Users need the flexibility and knowledge to optimally choose from available radios. Users should be discouraged from purchasing radios that would be neither operationally undesirable, problematic, cost prohibitive, nor declared “end-of-life” radios. Users are prohibited from using radios or accessories that may be destructive to the system.

Protocol
Before a new radio or certain accessories are approved for use it must undergo testing on the system. Radio Communications is responsible to conduct actual radio tests. Once sample radios or accessories are obtained, the testing process shall be completed as quickly and efficiently as practical so as to not delay the availability of new radios to users.

Radios removed from the system for decommissioning purposes shall be deprogrammed so as to remove all system related information, ID’s, and conventional channels, leaving only an idle frequency of 851.0000MHz to prevent potential interference issues with public-safety communications.

Management
Radio Communications is responsible for managing this process including maintaining all testing and certification records, managing radio equipment manufacturer initiated submittals, coordinating activities of the test team, and the proper deprogramming of subscriber radios. The Radio Communications Manager’s office maintains and has available a list of all radios approved for use on the system along with any limitations on use of the radio, its features or accessories.

4.14 System Administrator Standards

Purpose or Objective
Establishes the minimum training standards for system administration and staff. This ensures that system functionality and integrity are maintained by restricting system administrative functions to trained, qualified and authorized personnel only.

Operational Context
System functionality and integrity shall be maintained by ensuring that only qualified personnel perform system administration functions.

Protocol

Radio Communications is responsible for maintaining system configuration databases for system or subsystem infrastructure, subscriber databases and console configuration databases. Therefore, the Radio Communications Manager shall ensure that any personnel with access to those databases shall have successfully completed the appropriate training and demonstrated proficiency on the system management functions or be closely supervised by approved trainers.

Appropriate training shall, at a minimum, include formal factory training or training conducted locally by a qualified factory trained instructor.

- In addition, personnel responsible for the day-to-day database administration (i.e., any modifications or additions to a system or subsystem subscriber database) are trained at formal factory training or by a properly trained system or subsystem administrator.
- System access rights are not given to personnel who have not had the proper training or demonstrated proficiency.
- Radio Communications shall maintain a list of training completed by technical staff.

Procedure

This SOP does not contain specific training procedures or training modules.

Management

The Radio Communications Manager's office is responsible to ensure that:

- An appropriate training plan is developed for all technical and administrative staff
- Minimum training requirements are met
- Only qualified personnel perform system administration functions
- System administrators are familiar with all applicable sections of the System Standards Manual

4.15 Technical Staff Training

Purpose or Objective

Establishes the minimum training standards for system technical staff to ensure system functionality and integrity is maintained by requiring system maintenance functions to be performed by qualified personnel.

Operational Context

System functionality and integrity shall be maintained by ensuring that only qualified personnel perform system maintenance functions.

Recommended Protocol

Any Agency's technicians or vendors' technicians that will be working with the system infrastructure shall be manufacturer trained radio technicians. System technicians are required to hold at least one of the following industry recognized technician certifications or licenses:

- FCC General Radiotelephone Operators License
- APCO Public Safety Technician Certification

Any Agency's technicians or vendors' technicians that will be working with the subscriber units or control stations shall be trained radio technicians. All radio technicians should receive regular, formal manufacturer's training.

Technicians assigned to work on the infrastructure and/or subsystem equipment shall successfully complete appropriate training on all such equipment. Appropriate training shall, at a minimum, include formal factory training either at the factory or on-site, conducted by a qualified instructor or in the field with a qualified technician. If factory training does not exist for a component of the system, the technician shall become familiar with the technical documentation and receive on-the-job training from experienced technicians on the equipment.

- In addition to training requirements for in-house technical staff, any technical staff from contracted service providers shall also meet the minimum training requirements for the equipment they are assigned to work on.

- Personnel employed by contracted maintenance or outside service providers will be subject to a background investigation prior to performing any work on System components.

- Untrained and uncertified personnel shall not perform any maintenance or repair work unless this work is performed under the direct supervision of a trained and certified technician.

- Infrastructure systems and subsystem technical staff shall remain familiar with the site access procedures, equipment outage and maintenance notification requirements of this standards manual.

- Radio Communications shall maintain a list of technical training completed by administrative and technical staff.

Other training/certifications that Agency's radio technicians should have include:

- Communications Unit Leader (COML)
- Communications Technician (COMT)
- ICS courses 100, 200, 700b, 800 and others as required by employing agency
- Training on deployment and operation of Mobile Communications Units
- Any other developmental, technical or safety courses deemed necessary by the agency

Procedure

This manual does not contain specific training procedures or training modules.

Management

The Radio Communications Division Manager is responsible to ensure that:

- Minimum training requirements are met
- Only qualified personnel perform system maintenance functions
- System technicians maintain familiarity with all applicable sections of this manual
- An annual review of staff skills is performed and appropriate training is planned based on those reviews

4.16 Communications / 9-1-1 Center Personnel Training

Purpose or Objective

Establishes minimum training standards for public safety communications /9-1-1 center personnel with access to System resources. This ensures that personnel performing communications dispatch operations are properly trained.

Operational Context

System functionality and integrity shall be maintained by ensuring that only qualified personnel perform dispatch functions.

Protocol/ Standard

- Public safety communications /9-1-1 center personnel shall successfully complete appropriate training on the console system. Appropriate training shall, at a minimum, include formal training either by a public safety communications trainer who has completed the training from a qualified instructor or by a qualified factory instructor familiar with the agency's operations.
- Public safety communications / 9-1-1 center personnel shall be familiar with all applicable mutual aid requirements, interoperability requirements, trunk system patching and all established SOPs.
- Other recommended manager / supervisor training / certifications that each Agency's communications center personnel should have include:
  - COML
  - ICS courses 100, 200, 700b, 800 or others as required by employing agency
  - Any other developmental, technical or safety courses deemed necessary by their employing agency

Recommended Procedure

This policy does not contain specific training procedures or training modules.

Management

The communications / 9-1-1 center Manager within each agency is responsible to ensure personnel with radio console access to resources on the System comply with the following:

- Public safety communications / 9-1-1 center personnel receive the appropriate training before accessing System resources

- Public safety communications / 9-1-1 center personnel maintain familiarity with features and functions of communications consoles in order to rapidly and effectively communicate with public safety personnel and are able to identify and establish interoperability solutions when appropriate or directed
- Only qualified personnel perform dispatch functions on System resources
- Public safety communications / 9-1-1 center personnel maintain familiarity with all applicable sections of the system standards manual

4.17 Incident / Tactical Dispatcher / RADO Training

Purpose or Objective

Establishes minimum training standards for those performing incident / tactical dispatch / radio operator (RADO) functions with access to System resources. This ensures that system communications tactical dispatcher / RADO operations are performed by properly trained incident / tactical dispatch personnel.

Operational Context

System functionality and integrity shall be maintained by ensuring that only qualified personnel perform incident/tactical dispatch functions.

Protocol or Standard

- Incident / tactical dispatch personnel shall successfully complete appropriate training on the console system, mobile radios or control stations in the Mobile Command/Communications Units. Appropriate training shall, at a minimum, include formal training either by an incident/tactical dispatch trainer who has completed the training from a qualified instructor or by a qualified radio technical staff member familiar with the Mobile Command/Communications Units' (MCU) operations.
- Incident / tactical dispatch personnel shall be familiar with all applicable mutual aid requirements, interoperability requirements, trunked system patching, gateway and other communications equipment in the MCU as well all established standard operating procedures.
- Other recommended incident / tactical dispatcher training / certifications that each agency's incident / tactical dispatchers / RADOs should have include:
- COML
- COMT
- ICS courses 100, 200, 700b, 800 or others as required by their employing agency
- Any other developmental, technical or safety courses deemed necessary by employing agency

Procedure

This policy does not contain specific training procedures or training modules.

Management

The Communications Center Manager within each agency is responsible to ensure personnel with access to MCU resources on the System comply with the following:

- incident / tactical dispatch personnel or those acting in that capacity receive the appropriate training before accessing System resources
- incident / tactical dispatch personnel maintain familiarity with features and functions of MCU in order to rapidly and effectively communicate with public safety personnel and are also able to identify and establish interoperability solutions when appropriate or directed
- only qualified personnel perform incident/tactical dispatch functions on System resources
- incident / tactical dispatch personnel maintain familiarity with all applicable sections of the system standards manual

4.18 Radio (Subscriber) User Training

Purpose or Objective

Establishes the minimum training standards for radio users, which ensures proper operation of radios on the system.

Operational Context

System functionality and integrity shall be maintained by ensuring that only trained personnel operate radio equipment.

Protocol/ Standard

- Radio users shall successfully complete appropriate training on assigned radios before being allowed to operate on the system. Appropriate training shall, at a minimum, include formal training from a qualified instructor or approved media.
- Radio users shall be trained on the technical operation of assigned radios.
- Radio users shall be trained on how to operate the radio within the System along with any special features of the system they will use, e.g. interconnect, private call, etc.
- Radio users shall be trained on and demonstrate proficiency with all applicable mutual aid and interoperable communications resources and standard operating procedures.
- Radio users shall maintain awareness of the mutual aid, interoperability channels or talkgroups in their radios, as well as how to navigate to them when necessary.
- User agencies will make an effort to conduct on-going refresher training for radio users periodically following their initial training (e.g., build into in-service training, dispatch centers conduct random tests, roll call training, on-shift training, etc.).
- Radio Communications staff assists user agencies in identifying training needs and implementing training programs to meet those needs.

Procedure

This manual does not contain specific training procedures or training modules; however, Radio Communications staff assists with radio user training when requested.

Management

Each User Agency is responsible to ensure that:

- Personnel assigned radios shall receive the appropriate training with emphasis on awareness of and how to navigate to mutual aid and interoperability channels or talkgroups (initial and on-going refresher).
- Only trained and qualified personnel shall operate radio equipment.
- Radio users are familiar with all applicable sections of the system standards manual.

4.19 Interoperability and Non-Metro Radio Users

Purpose or Objective

Establishes the minimum training standards for radio users having access to interoperable talkgroups of the System. This ensures the proper operation of radios on the system and safeguards against improper utilization of interoperability resources.

Operational Context

System functionality and operability is maintained by ensuring that only properly trained personnel use the interoperable talkgroups on the System for interoperable/mutual aid communications. If non-participating agencies do not have appropriate training, then communications system failure or a degradation of system resources may occur.

Protocol/ Standard

- Interoperable radio users shall have:
    - successfully completed appropriate initial and on-going refresher training
    - demonstrated knowledge of Section 6 Interoperability Standards
- The end user training emphasizes:
    - the use of interoperable channels and how to navigate their radio
    - how a non-participant's radio experiences are affected by the digital System
- The dispatch and supervisory training emphasizes:
    - the use of interoperable channels
    - the use of patching and patched channels
    - the use of cross band repeaters and gateway devices
    - the use of RF control stations
    - how a non-participant's radio experiences are affected by the digital trunked radio system

Radio users with access to interoperable channels must be familiar with all applicable mutual aid and interoperable requirements and procedures.

Procedure

This manual does not contain specific training procedures or training modules.

Management

The Radio Communications Subscriber Support office will provide training materials for initial and on-going refresher training. Additionally, as resources permit, the Radio Communications Manager's office will assist user agencies with developing plans and methods of incorporating on-going radio refresher training into various activities for the most effective delivery to personnel.

Agencies requesting and/or using the interoperable talkgroups are responsible to ensure that:

- The use of mutual aid / interoperability channels / talkgroups is properly coordinated and approved through a Communications Coordinator (COMC), COML, Communications Center Dispatcher/Supervisor, or Incident Commander.
- Radio users successfully complete appropriate initial and on-going refresher training and demonstrate knowledge of proper communication procedures before being allowed to operate the interoperable talkgroups.
- Radio users are familiar with all applicable interoperable sections of this manual.
- Radio users are familiar with all applicable mutual aid requirements and interoperable SOPs.

4.20 User Feedback

Purpose or Objective

Establishes procedures for users to provide constructive feedback relating to system operations and usage.

Protocol/Standard

As events and incidents occur, radio users may find areas, procedures, and/or other issues that impede or hamper reliable radio communications. These issues should be reported to MRC for investigation and correction as necessary.

Recommended Procedure

MRC staff shall be notified immediately upon recognition of problems with radio communication, whether they are operational, procedural, mechanical, or coverage related. After Action Reports detailing specific communications issues should be forwarded to the MRC Division Manager for follow-up.

MRC will interview those affected to determine the scope of the problems and develop and implement a corrective plan of action.

Management

The Radio Communications Manager will be responsible for the oversight and compliance of this standard.

4.21 System Upgrades

Purpose or Objective
Establishes notification procedure prior to system upgrades

Protocol/Standard
System software upgrades will be performed on a bi-annual basis beginning in 2016 or as needed contingent on funding by the Metro Council.

All agencies using the System will be notified at least 30 days prior to a major system upgrade that will cause a system or site outage. Any user agency must notify MRAM in writing if this would interfere with any major planned events or exercises.

All outside agencies using the System must have governance agreements in place to address the timing of system upgrades and associated costs.

Recommended Procedure
Radio Communications staff will be responsible for sending out a written notification or email to all System user agencies and system users / Zone managers that may be impacted by the upgrade.

4.22 In-building Coverage (Bi-Directional Amplifers)

Purpose or Objective
Establishes policy on usage of Bi-Directional Amplifiers (BDA)

Technical Background
The system is designed for mobile and portable radio coverage

Protocol/Standard
It is not the intent for MRAM to approve or regulate BDA's. It is important for Radio Communications to maintain a list of facilities that do have BDA's used with the System.

Any agency or department installing a BDA will send in the location of the device prior to installation if possible. This will include the physical address, building name, location within the building, Manufacturer and model number.

It is the responsibility of the equipment/facility owner to comply with all requirements of the FCC, including licensing, location reporting, and interference mitigation.

Recommended Procedure
Entities installing BDA will submit to MRAM a list of locations where BDA's are installed that are supplementing the System. BDA's not supplementing the System do not need to be reported. This list will be update periodically.

Management
Radio Communications staff will maintain the BDA list.

4.23 Aircraft Radio Installations and Operation

Purpose or Objective
Sets the policy regarding aircraft subscriber radio installation, programming, and operation on the System.

Technical Background
Due to the elevated altitude of operation, aircraft radios have a greater coverage footprint. This allows a radio operated in the air to talk into sites as far away as 150 to 200 miles, while mobile radios operated in vehicles on the ground typically have ranges limited to 30 to 40 miles. Radios in aircraft operating with the System function slightly different than radios on the ground.

Due to the interference potential from the larger coverage footprint of aircraft operated radios, the FCC rules for operation of these radios limits the output power to help reduce interference, as frequency reuse is applicable in Metro's system and other radio systems.

Installation of aircraft mounted radios is governed by the Federal Aviation Administration (FAA) and permanent installations must be performed by FAA certified personnel.

Operational Context
Subscribers that acquire a large coverage footprint due to high altitude operations need to take the following into consideration:

- Potential interference due to frequency reuse in other systems using the same frequencies. This could cause interference to their users. This interference could appear as an interruption, or loss of communications, or as tailgating to other talkgroup transmissions on other sites.

Protocol/Standard
All permanently installed aircraft radios shall comply with the FCC 90.423 power output limitation of 10 watts, the ERP no more than 5 watts. Only unity gain antennas will be allowed.

Permanently mounted aircraft radios should be programmed with the following:

- BER threshold of 2.5%

For aircrews that are assigned portable radios, these portable radios should be programmed for the following:

- 2.5% or 2.9% BER threshold

These settings apply for both aircraft installed radios using remote mounted mobile or portable radios and Technisonic-type aircraft control panel mounted avionics packages using internal portable radios.

Procedures for landing zone areas where communications with ground personnel are conducted are recommend on a simplex, non-trunked, channel.

In addition to the SOP training requirement, training for users of aircraft radios shall include a description of the issues surrounding airborne operation of System radios:
(1) Issues of potential interference to other system users due to frequency reuse;
(2) Personnel using portable radios in a limited capacity (observers, guests, etc.) and the potential for FAA and FCC rule violation, and interference.

Recommended Procedure

Installation and programming should be performed as outlined in this section.
Operation of Aircraft landing zone coordination should be performed as outlined in this section.
In-flight transmissions should be as brief as possible due to the potential interference.

Management

The Radio Communications Manager will be responsible for the oversight and compliance of this standard. Due to the potential of interference issues to expand beyond a specific region or into another state, Radio Communications staff should also be notified if any interference is detected and is believed to have originated from an 800MHz Radio System equipped aircraft.

4.24 Change Control

Purpose or Objective

To ensure that all significant changes to the system's configuration are reviewed and tracked in a controlled and coordinated manner. It reduces the possibility that unnecessary changes will be introduced to the system without forethought.

Technical Background

Change control is currently used in various products and systems. Typical examples from the computer and network environments are patches to software products, installation of new operating systems, upgrades to network routing tables, or changes to the electrical power systems supporting such infrastructure.

Operational Context

A formal request is generated for something to be changed and is reviewed by the Metro ITS Change Management group before the requested changes are implemented.

Protocol/ Standard

The Change Management group will make a risk analysis both to the system and to the process, and follow this by making a judgment on whether to proceed with the change as submitted. If the change requires more than one type of assessment, the head of the change control team will consolidate these. Everyone with a stake in the change should be aware of the request and determine whether there is a business or technical justification for the change.

Management

The Radio Communications Manager is responsible for seeing that the Change Control process is followed.

5.0 CONFIGURATIONS AND ALLOCATION

5.1 Naming Standards

Purpose or Objective

Establishes the method which determines a unique agency alias or acronym for individual agency's radios in order to ensure that there are no duplicates and to facilitate intuitive understanding of the alias as it relates to the agency's name.

Technical Background
Every radio user ID in the system shall be unique. There can be no duplicate IDs. The radio user alias field holds up to 14 characters and the valid values that the system can accept are: upper case alpha, numeric, period, dash, forward slash, and number sign.

Operational Context
With the exception of the first few characters, users are technically free to choose any unique name. However, since this is a shared system, radio user aliases that are programmed into the system shall adhere to the established naming conventions for agencies that will not conflict with each other.

Protocol/ Standard
In order to meet this need, the radio user aliases are prefixed with an agency identification that is unique to that agency and logically identifies the agency and the associated radio user (e.g., P for Police, F for Fire, N for NES, SCH for Schools, PW for Public Works, etc…).

The naming standard for most agencies only govern up to the first three characters. The characters following the first three are at the individual agency's discretion, for example, the agency can opt to internally use more than two characters for the internal identifications.

The body of the alias contains an agency's identification for the individual, pool or cache radio etc., possibly the radio user's call sign or employee number as an example. If a radio user has multiple radios on the system, each radio shall have a unique alias. The alias shall be suffixed with identification for the radio itself, such as an "M" for a mobile radio, and a "P" for a portable to differentiate between a mobile & portable radio used by the same person. This allows dispatchers and Radio Communications staff to readily identify radio users and whether the radio is a portable or a mobile.

A master list of radio user aliases is maintained in the system and the naming prefix template is maintained by MRC. Radio user aliases are readily accessible through the data terminal. As alias names are created and approved, they shall be placed on the master list for operations and planning.

As new agencies are added to the System, the Radio Communications staff shall assign an agency identification prefix in accordance with the naming convention established within this SOP.

Management

The Radio Communications Subscriber Services office shall maintain the current radio user alias assignments. All System users are responsible for following and maintaining the defined standard.

5.2 Radio Zones Naming

Purpose or Objective

Establishes the standard by which all agencies on the radio system use a zone acronym to precede the talkgroup names in order to ensure no duplicates, and to facilitate intuitive understanding of the acronym relating to the zone and agency name.

Technical Background

All talkgroup names programmed in the system must be unique and there can be no duplicates. Depending on the radio type and/or model the talkgroup name field holds from 8 to 12 characters. This number is further limited by the need to identify the different zones assigned to an agency. Because of this need it is recommended that the first 1 or 2 characters be used to identify the particular zone, if feasible. (e.g., if the zone name identifier is 3 characters, the channel or talkgroup name length is reduced by 3 characters)

Operational Context

The zone acronym reasonably identifies the primary talkgroup user whenever possible, with multiple zones using sequential numbering. For example: “P101WSTD” would represent Police, Zone 1, Talkgroup 1, West Dispatch, while “FB1_DISP” represents Fire Dept. Zone B, talkgroup 1, Main Dispatch. In some cases a longer acronym may be required to identify agencies with similar names or initials, which is acceptable as long as the same scheme is used across the system.

Protocol/ Standard

The zone aliases are prefixed with an agency identification that is unique to the agency and is assigned by Radio Communications e.g. P=Police, NES=Nashville Electric Service, OEM=Office of Emergency Management, PW=Public Works, etc.

The naming standard governs characters 1-3 for most agencies. Characters following the zone acronym are at the individual agency’s discretion

A master table of zone aliases is maintained by Radio Communications. As alias names are created/changed they are placed on the master list and are available on request to all appropriate parties for operations and planning.

Management

Radio Communications is responsible for seeing that the defined standard for zone naming is followed and maintained.

5.3 Talkgroup Naming

Purpose or Objective
Establishes a standardized and common naming convention for talkgroup identification across the System.

Technical Background
The number of characters shown on the display on a radio will vary depending on the manufacturer type and/or model. Some radio models may not be capable of displaying more than 8 characters.

Operational Context
It is essential that all users of the System follow the same naming standard because some talkgroups are shared by multiple agencies. With the exception of the assigned prefix, talkgroup owners are technically free to choose any unique name they wish for their talkgroups. However, since this is a shared system, talkgroups that are programmed into radios shall have naming conventions that will not conflict with other agencies.

Failure to utilize common talkgroup naming can result in lack of ability to communicate across agencies as users may not recognize they have talkgroups in common if they are named differently.

Protocol/ Standard
The talkgroup name (alias) shall be prefixed with a short acronym that identifies the agency that owns the talkgroup. The agency prefix is assigned by MRC staff and shall be identified on the “Agency Naming Prefixes” table maintained by MRC.

Some talkgroups are not owned by an individual agency and will not have an agency specific identifying prefix. Examples of these are network wide mutual aid talkgroups, or those set aside for interoperable communications, incident command, or special events.

Talkgroups shall use the same name (alias) in all radios and consoles when possible; however, due to radio programming limitations, some models of radios are not capable of displaying more than 8 characters. These radios require condensing the talkgroup name to fit within the radio programming capabilities.

Standard talkgroup names will be utilized as follows:

- programmed into all subscriber radios
- programmed into cache radio equipment
- programmed into Mobile Communications Vehicles (MCV)/MCUs and other transportable communications equipment
- communications Center Consoles and control stations
- when written in any type of documentation such as SOPs, Communications Plans (ICS205), Incident Action Plans (IAPs), Communications Resource Availability Worksheets (ICS Form 217A)

This standard allows radio users, dispatchers and Radio Communications staff to readily identify talkgroup ownership.

Talkgroup name changes must be approved by the Radio Communications Manager in order to maintain continuity.

Management
Radio Communications staff is responsible to ensure that the defined standard is followed and maintained.

5.4 Talkgroup Assignment, Activation, and Deactivation

Purpose or Objective
Allocates talkgroup ID ranges for individual agencies. This allows agencies and Radio Communications to manage the pool of IDs as talkgroups are configured. This simplifies the management of the IDs and provides an easier indication of agency IDs. There are a limited number of ID's within a system.

Technical Background
System talkgroup ranges are assigned according to the primary zone.

Operational Context
Talkgroups will be assigned, activated, and deactivated by the Radio Communications Manager based on agency need and available system resources.

Protocol/ Standard
Individual agencies may only use the talkgroup IDs assigned to them by Radio Communications for programming their subscriber equipment or those of other user agencies for which they have received written authorization.

Any agency that has unused talkgroup IDs should notify Radio Communications in writing that they are returning unused talkgroup IDs. If for some reason the agency relinquishing the IDs needs additional talkgroup IDs in the future they may submit a request.

MRAM reserves the right to audit Talkgroup usage. Any talkgroup IDs that have not had any activity for over one year may be reclaimed for future usage. Radio Communications will notify the assigned agency of pending revocation. If for some reason the agency relinquishing the IDs needs additional talkgroup IDs in the future they may submit a request.

Procedure
Agencies needing talkgroup allocation shall submit a written request to Radio Communications for review and approval prior to resources being assigned. Agencies should provide reasonable justification in their written request for individual talkgroups, along with any requirements such as encryption or special functions.

Management
The Radio Communications Subscriber Support Office manages the ID ranges for day-to-day activities and for reserve allocation.

5.5 Radio ID Allocation

Purpose or Objective
Allocates radio ID ranges for the individual agencies. This allows the individual agencies and Radio Communications to manage the pool of IDs as radio users and console positions are configured. This simplifies the management of the IDs and provides an easier indication of what IDs belong to which agency in the event that a radio user alias is not available.

Technical Background
The System will recognize any radio ID less than the numerical value of one million, but the system is currently limited to a total of 128,000 IDs.

These IDs are the same IDs that users type in for private calls or call alert pages. Also, the IDs picked at this step are the same IDs that are displayed on the subscriber radios if the "ID Display" feature is enabled. These IDs are also displayed at the console if the console alias feature is not available.

Operational Context
The Radio Communications Subscriber Support Office will allocate specific radio ID ranges to specific agencies and talkgroups based on the number of units the agency will have active the system and will be shown on the master agency alias list.

Protocol/ Standard
For programming radio users and console positions, individual agencies can only use IDs reserved for them in the agency alias list.

Any agency that has radio IDs they are not using nor anticipate using should notify Radio Communications in writing that they are returning unused radio IDs. If for some reason the agency relinquishing the IDs needs additional radio IDs in the future they may submit a request.

MRAM reserves the right to audit radio ID usage. Any radio IDs that have not had any activity for over two years may be reclaimed for future usage. The Radio Communications Subscriber Support Office will notify the assigned agency of pending revocation. If for some reason the agency relinquishing the IDs needs additional radio IDs in the future they may submit a request.

Procedure
There is a reserve pool of ID numbers for agencies that need an additional allocation or for new agencies as they come onto the system. In this case the agency shall make a written request to Radio Communications for review. The request should include how many ID’s

are requested, justification and a time table for them to be placed into service. The Director may approve, deny or request additional information.

Management
The Radio Communications Subscriber Support Office manages the ID ranges for day-to-day activities, and manages the ID ranges for reserve or future allocation.

5.6 Fleetmap Standards

Purpose or Objective
Defines the process used to document the fleetmap information for the effective management of the system. This information is in a format that can be shared with all agencies. This provides a resource for subscribing agencies to reference when planning interagency communications. System fleetmap configuration information is classified as confidential and is not released to the public.

Technical Background
The fleetmap is parameter information programmed into the system infrastructure and into the subscriber radios to control how those radios perform on the System.

The fleetmap spreadsheet is a documented matrix of the talkgroups in the system and the departments or agencies that use and control user access to these talkgroups. The fleetmap contains the following information:

Talkgroup Name	Name of the talkgroup as it is programmed into the system
Talkgroup Alias	Abbreviated naming of the talkgroup to fit within the 8 or 14 character radio display
Talkgroup ID	Numerical designation of the talkgroup in decimal and/or hexadecimal
Failsoft Channel	The system channel designated for the talkgroup when in the failsoft mode
Owner	The primary user agency with access control of the talkgroup
Priority	Priority level of the talkgroup
On Console	If the talkgroup is available as a console resource
Sharing	The level of shared access as described in Section 5.9, ‘Talkgroup Sharing’
Emergency Backup	A talkgroup to be used when the user’s primary system is unavailable

Access is tightly controlled and is considered ‘Restricted Information’.

Operational Context
The Radio Communication Manager is responsible for managing the fleetmap information of the users. The ID information is kept secure as described in Section 8.

Protocol/ Standard

A detailed matrix is maintained on the system database. Each agency's radio representative maintains a fleetmap spreadsheet containing data on their talkgroups and the users for whom they are responsible.

Procedure

- If individual agency representatives desire to make updates and changes to their spreadsheets, the changes shall be coordinated with Radio Communications. This allows Radio Communications technicians to document any updates, coordinate those changes that affect other agencies and/or users and maintain the databases for reference and interagency fleetmap planning.

- Talkgroups that are shared between subscribers of different agencies must be reflected on all the spreadsheets having subscribers using these talkgroups.

- Radio Communications, at the direction of the talkgroup owner agency, may omit listing any information in the master fleetmap spreadsheets for encrypted talkgroups used for undercover operations and other highly sensitive activities. Unless specifically provided for elsewhere, all other system standards apply to the use of encrypted talkgroups.

- The disclosure of the fleetmap configuration information including talkgroup IDs, user IDs, user privileges and other related system information could substantially jeopardize the security of the system. This disclosure makes it more susceptible to tampering, sabotage, unauthorized use, jamming, hacking, unauthorized access to the contents of confidential voice and data communications. Therefore, the master fleetmap spreadsheets shall be classified as 'Restricted Information' and are not available to the general public except by formal written request to MRAM.

Management

Radio Communications manages the fleetmap and radio system programming for all agencies and the details of the process for communicating the information.

5.7 Subscriber Template Management

Purpose or Objective

Defines the process that is used to document the radio subscriber template information for the effective management of the system. The System contains a large number of talkgroups to support the various agencies that subscribe to the system. Subscriber template configuration information is classified as 'Restricted Information' and is not released to the public.

Technical Background

The subscriber template is parameter information programmed into the individual subscriber radios to control how those radios perform on the System.

An agency's subscriber template spreadsheet is developed and maintained by Radio Communications or that agency's radio service shop with the input of each agency's radio representative. This is to ensure the agency gets the talkgroups, features, and functionality desired from the radios, while maintaining the overall functionality and integrity of the radio system.

The radio subscriber template is usually specific to a particular agency but an agency can elect to have different versions of the template based on the department's needs and operations.

The templates normally contain the following information:

Radio Configuration	Specific information related to a particular model of radio, including but not limited to; button assignment, display options, menu items, and other radio wide parameters
Conventional	Personality information that determines the radios' operation in the conventional mode such as frequencies, tones, and signaling options
Trunking	Identifies systems and talkgroup specifics that the subscriber radio has access to, as well as system and unit specific ID numbers relating to the radios operation
Scan	Defines the limits and lists of the subscriber radio's scan function, when equipped
Zone Assignment	Where talkgroups are combined into specifically labeled 'zones' within the radio that represent or reflect operations of a particular agency or operation. The zone designation reflects an acronym, which should easily identify the zone as belonging to a particular agency.

Operational Context

The Radio Communications Subscriber Support Office is responsible for managing the subscriber template information of the users. The ID information is kept secure as described in Section 8.

Protocol/ Standard

The Radio Communications Subscriber Support Office and each agency's radio representative shall maintain a subscriber template spreadsheet for each of the agency's template versions.

Metro Radio Communications must review and approve all subscriber templates before they can be programmed into a radio. Any agency, vendor, or contractor that develops radio templates for use on the System must submit them to MRS for approval before they can be activated on the System. Any entity that places an unapproved template into service on the system is subject to losing their programming privileges and/or system access.

Procedure

If individual agency representatives desire to make updates and changes to their templates, those changes shall be coordinated with Radio Communications. This allows the technical staff to document any updates, coordinate those changes that affect other agencies and/or users, and maintain the database for reference and interagency fleetmap planning.

The Radio Communications Subscriber Support Office, at the direction of an agency using encryption, may omit listing any information in the master fleetmap spreadsheets for encrypted talkgroups used for undercover operations and other highly sensitive activities.

The disclosure of the template configuration information including talkgroup IDs, user IDs, user privileges and other related system information could substantially jeopardize the security of the system. This disclosure may make it more susceptible to tampering, sabotage, unauthorized use, jamming, hacking, and unauthorized access to the contents of confidential voice and data communications. Therefore, the master fleetmap spreadsheets shall be classified as 'Restricted Information' and are not available to the general public except by formal written request to MRAM.

All subscriber programming templates must be submitted to and approved by MRC staff before use on the system.

Management

The Radio Communications Subscriber Support Office manages the fleet mapping, subscriber templates, and radio system programming for all agencies and the details of the process for communicating the information. Access is tightly controlled and is considered confidential.

5.8 Talkgroup Ownership

Purpose or Objective

Defines the ownership of private, shared, and interoperable talkgroups and resources, and provides a standard so that Radio Communications shall have firm guidelines on allowing particular talkgroups programmed into radios.

Operational Context

Talkgroups are considered 'owned' by the agency requesting the creation of the talkgroup. The process for pre-defined sharing authorizations is explained in Section 5.9.

Recommended Protocol/ Standard

There are three tiers of talkgroups that are programmed into the system:

Private:
Private talkgroups are owned by the individual user agencies, are used for normal day-to-day operations, and are not shared with any other agency. These talkgroups are prefixed with the owning agency's identification as defined in the talkgroup naming standards of the system standards manual.

Private talkgroups are either "Listed" or "Unlisted". Only those private talkgroups used for undercover operations or other highly sensitive confidential law enforcement activities shall be "Unlisted".

Shared:
Private talkgroups are owned by the individual user agencies, and shared with other agencies by mutual agreement. These are generally used for routine or pre-planned activities between the sharing agencies.

Talkgroups are prefixed with the owning agency's identification as defined in the talkgroup naming standards of the system standards manual.
Private and shared talkgroups are "owned" by a particular agency or group of agencies and the talkgroup shall not be programmed into other agency's radios unless specifically authorized by the "owner". Radio Communications shall not allow a talkgroup to be programmed into a radio without such authorization.

Before a talkgroup can be shared, the owning agency must "pre-authorize" the sharing arrangement and/or provide a letter of authorization.

Interoperable:
Interoperable (e.g. Unified and Incident Command and Mutual Aid) talkgroups are intended for interagency communications and assistance and fall into two categories: 1) those used for System communication only, and 2) those that are patched to conventional or other trunked system RF resources.

Interoperable talkgroups shall not be owned by any specific agency but may require letters of authorization from MNPD, Metro Fire, and OEM. The authorizations are defined in Section 6 of this manual. This provides standing written documentation so that Radio Communications has firm guidelines on allowing particular talkgroups in radios.

Because these are non-owned talkgroups, talkgroup names shall not be prefixed with agency identification.

Procedure
Radio Communications technical staff will control all talkgroup generation and access parameters. Talkgroup owners shall immediately notify Radio Communications when changes to an owned talkgroup are required or the talkgroup is no longer required. The procedure regarding pre-authorizing talkgroup sharing is defined in Section 5.9 of this manual.

Management
Radio Communications staff is responsible to see that this policy is implemented as defined in this system standards manual. Identified issues and concerns shall be sent to the Technical Committee for resolution.

5.9 Talkgroup Sharing

Purpose or Objective

Defines how talkgroup owners permit access to outside users when requested and if desired provides an option to the users of the System that allows discretion to the talkgroup owners to predefine sharing authorizations for other agencies.

Technical Background

Radios must be compatible with the signaling format of the system**.** Radios that are not P25 capable will not be able to access talkgroups on the System.

Operational Context

Talkgroups are considered 'owned' by the agency requesting the creation of the talkgroup. As the owner of the talkgroup the agency has the authority and control to define who is allowed access to the talkgroup and to what degree. All talkgroups are considered as private unless specifically identified in writing to Radio Communications as a shared resource and with whom it can be shared. This process is accomplished with a formal written request to Radio Communications from the requesting agency which is passed to the talkgroup owner for approval.

The suggested method to simplify this process is for the owning agency to predefine a shared radio zone with all of the talkgroups allowed assigned therein.

Predefined zones are kept in the talkgroup spreadsheets maintained by Radio Communications. These spreadsheets are a reference available for the users of the system for talkgroup planning. If an agency does not pre-define a shared zone or talkgroup, then specific authorization for a particular talkgroup must be obtained from the talkgroup owner.

Protocol/ Standard

The following letter designators are used to define the intended pre-authorizations in the master fleetmap:

C	Controlled Access: Permission is required to gain authorization for use; a letter of permission must be generated and on file with Radio Communications for each agency, entity, or individual user's authorization
I	Interoperability: Access allowed for purposes of interoperable communications; these talkgroups are often found in pre-authorized zones and are shared with like agencies e.g. law, fire, med, etc.

If a talkgroup has not been assigned a level of pre-authorization, by default, it is considered private.

Procedure

Radio Communications, working with the talkgroup owners, performs the task of assigning talkgroup sharing designations in the master fleetmap and ensuring those levels of access are reflected in the appropriate subscriber templates. If a talkgroup has not been assigned a level of pre-authorization, it is considered private.

Management

The Radio Communications Manager is responsible for the management of this procedure.

5.10 Talkgroup and Radio User Priorities

Purpose or Objective
Establishes varying priority levels for talkgroups to assure the most critical talkgroups on the system are granted a channel as quickly as possible when the system is experiencing busy conditions.

Technical Background
The system priorities can be managed both at the radio user level and at the talkgroup level.

Operational Context
Priority levels in the system are managed at the talkgroup level. The goal is to distribute priorities across the systems talkgroups in a way that maximizes the ability for critical groups to communicate and minimizes the number of talkgroups with high priority. All radio user priorities are set to the lowest priority level, 10. As radio users change talkgroups, the effective priority is set by the assigned talkgroup.

Protocol/ Standard
Radio Communications assigns talkgroup priority levels not exceeding the level defined by the criteria below. Talkgroup priorities that are assigned to level five or above are subject to the review and audit provisions that are specified in Section 5.4 of this SOP.

Priority 1:
[EMERGENCY]: Only Emergency Alert calls, i.e. emergency or 'Code 5000' button pressed, are given the Priority 1 status automatically by the system's controllers.

Priority 2:
[EXTRAORDINARY/TEMPORARY]: Is used for temporary re-prioritization (via system manager terminal) of a lower priority talkgroup for critical operations, i.e. presidential motorcade, major incident command, etc. In addition Priority 2 is assigned to dedicated "EMERGENCY ALARM" talkgroups for agencies such as Transit that do not use the Emergency Alert (emergency button) function.

Priority 3:
[UNASSIGNED]:

Priority 4:
[MEDICAL PRIORITY]: Is used exclusively for Ambulance to Hospital communication and coordination of medically related operations and information.

Priority 5:
[LIFE SAFETY AND PROTECTION OF LIFE AND PROPERTY]: Is used for talkgroups that have an impact on the delivery of services that involve the safety and the protection of life and property, including those talkgroups used by personnel involved in high risk and mission critical field operations.

Priority 6:
[NORMAL/ROUTINE PUBLIC-SAFETY COMMUNICATION]: Is for all talkgroups handling normal and routine public-safety agency communications for Metro agencies.

Priority 7:
[NON-MISSION CRITICAL]: Is for all other "secondary", "administrative", "non-essential" or "non-mission critical" talkgroups used by subscriber agencies, both public safety and general government. (See Glossary - Definitions and Acronyms for explanation of "Mission Critical" and related terms.)

Priority 8
[SHARED/MUTUAL AID]: Talkgroups normally dealing with system-wide mutual aid interoperable communications.

Priority 9:
[OUTSIDE AGENCY]: Is used by outside agencies talkgroups, where the agency is not a Metro or NES entity and has requested a dedicated talkgroup for their own use.

Priority 10:
[PRIVATE CALL]:
Is used for private calls as defined by direct point to point radio to radio communications that are not carried out within a talkgroup. This priority will also be used for talkgroups that are established for system testing.

Management
Radio Communications is responsible for supervision and management of this procedure.

5.11 Telephone Interconnect

The Telephone Interconnect feature is no longer used on the System due to the amount of resources it consumes.

5.12 Failsoft Assignments

Purpose or Objective
Creates and assigns system resources in a manner which maximizes system utility to new and existing users consistent with each user's mission and needs for radio communications.

Technical Background
When the main controllers detect certain failure conditions in the radio system, all available channels revert from a trunking mode into a conventional repeater type of

operation that is given the term 'failsoft'. During failsoft, talkgroups are assigned to a specific radio repeater if so programmed, which will allow the users to continue voice communication while repairs are made to the system.

There are a limited number of repeater channels available in the System, which causes a number of talkgroups to be combined on each channel while in failsoft. This requires the radio users to share those channels between numerous and often different disciplines and agencies. This congestion of radio traffic happens only during the failsoft condition.

If a talkgroup is not given a failsoft assignment, radios using that talkgroup will not receive any indication that the system is in the failsoft condition. This will result in loss of communications for any radio using that talkgroup without the operator's knowledge.

Operational Context

The radio programming template failsoft assignments are configured to balance the ability for users to achieve an acceptable level of communications while maintaining the individual agency's privacy when possible. While in the failsoft condition, all radios will display the word 'FAILSOFT' on the radio display and emit a short tone every 10-15 seconds to indicate to the user that normal trunked operation is unavailable.

Protocol/ Standard

It is the policy of MRAM to provide a failsoft assignment for every talkgroup in the system to prevent loss of communications for users. Under special circumstances this policy can be waived, but this requires a written request from the requesting agency, and careful coordination with Radio Communications staff.

Failsoft channel assignments are based on the needs of present users compared to new users consistent with each user's mission and need for radio communications.

The Technical Committee makes determinations concerning Failsoft channel assignments.

During a Failsoft condition, dispatchers may need to announce instructions to radio users and remind them that operations may be combined among several agencies and to implement radio discipline/reduced radio traffic.

Management

The Technical Committee is the responsible authority for failsoft issues.

5.13 Scanning

Purpose or Objective

Identifies operational procedures and responsible authorities governing scanning talkgroups, conventional channels or other trunked radio system activities.

Technical Background

The network infrastructure and subscriber units are configured to permit managed user scanning of talkgroups. Whether scanning is utilized in subscriber radios is at the option of the user agency. Including a talkgroup in a non-priority scan list does not necessarily result in the user hearing traffic on that talkgroup. Talkgroups are only active if there is at least one user affiliated who has the talkgroup of interest as their selected channel.

Subscriber units can scan a talkgroup, a talkgroup in another zone, a conventional radio channel or another trunked radio system if compatible. Scanning by multiple subscriber units can quickly overwhelm a trunked radio system creating system busies.

An entire radio can be set up as receive only. However, transmit capable radios cannot have individual talkgroups set for receive only. Any talkgroup programmed into a normal user radio is technically capable of both transmit and receive operation and any transmission can be displayed on a dispatch screen.

Operational Context

An 'owned' talkgroup shall be pre-approved by the talkgroup owner for monitoring privileges by others as shown in the 'Shared' column of the master fleetmap.

Protocol/ Standard

Before scanning and/or monitoring of owned talkgroups is allowed, permission shall be granted. Permission shall come from the jurisdiction/agency that is the "owner" of the requested talkgroup. Scanning shall also be approved by the radio user's agency or department radio representative in the template design before scanning will be available.

Procedure

Permission

If the talkgroup does not appear in the master fleetmap as pre-approved for monitoring, then permission shall be obtained in writing from the talkgroup owner.

Scanning Configuration

It is recommended that individual user scanning be limited only to specific talkgroups owned by the user's parent agency and only those others that require the user to respond in certain cases (i.e. a police officer monitoring fire dispatch for calls in his zone).

It shall also be noted that scanning is disabled when the user leaves the system and switches the radio to a conventional (non-trunked) channel such as the 8CALL90 channel.

Management

Radio Communications is the responsible authority for scanning issues.

5.14 Audio Logging Recorders

Purpose or Objective

Establishes the procedure for the use and accessing of audio logging devices.

Technical Background

A System Audio Logging Recorder allows all audio-based radio traffic to be recorded and stored for future reference.

Primary system audio is taken directly from the system and is stored on a hard-drive based recording system based at an agency's dispatch center.

A talkgroup does not need to be selected or active at a console position to be recorded.

Advanced Encryption Standard (AES) Encrypted calls are recorded, however, the encryption key is not installed into the system and therefore those recordings are unusable and unrecoverable.

Some models of Audio Loggers are capable of recording private calls.

Other options for logging recorder audio sources are console logging audio outputs and individual control station based systems.

- Console logging audio outputs include transmit audio, and select and un-select receive audio. Console logging audio is only available for talkgroups that are active at the console work position. There is no way in which the separate audio for a specific talkgroup can be identified as belonging to that specific talkgroup. There can be received audio on multiple talkgroups on the un-select logging recorder audio channel. Frequently the audio from more than one talkgroup can be mixed together resulting in the inability to understand any one of the mixed audios being recorded simultaneously.

- A control station can be used as a source to receive the audio from a specific talkgroup. Multiple control stations, one for each specific talkgroup to be recorded, can be used at any one recording location. Control stations could also be used to record encrypted talkgroups if properly equipped and with the correct encryption key.

Operational Context

Each agency needing to record their radio or telephone audio will decide where the primary system audio logger is installed, as well as which channels, talkgroups, or phone lines are configured to record.

Protocol/ Standard

An agency that needs to access the recording system or requires a copy of any logged radio traffic should make their request to the appropriate agency that "owns" the record. The request should include specific information detailing the talkgroup, radio user(s), radio ID, time of day, and any other information that would help in processing the request.

Individual agencies are allowed to purchase, operate, and maintain their own secondary logging systems for their own use, but access for those systems is limited to talkgroups specific only to those agencies unless otherwise approved by MRAM.

Each agency utilizing logging recorders to record audio from their agency's talkgroups is responsible for adhering to their internal procedures with regard to:

- Retention schedule for radio system recordings in compliance with State Records Retention requirements
- Responding to public records requests for copies of audio recordings for radio traffic on **THEIR** agency-owned talkgroups or channels
- Providing radio system recordings as requested by the judicial system
- Providing duplicate recordings upon request for internal agency use, investigative purposes, training, etc.
- Establishing a data storage and backup system for radio system audio recordings

Procedure

Requests for audio records should be directed to the specific agency Administrator managing the logging system.

Management

MRAM is responsible for this policy. Each agency is responsible for the operation and data back-up of their agency-owned logging system for their agency-owned talkgroups or interoperability talkgroups on their radio console. Shared non-owned talkgroups are the responsibility of any agency that uses it for a resource on their dispatch console.

5.15 Private Call

Purpose or Objective

Establishes the usage of the Private Call feature on the system. While this is a useful feature that is needed by some users, it shall be managed to an appropriate level to protect the primary radio communications purpose of the system and to preserve system resources.

Technical Background

Private calls can be placed between authorized individual users of the system. This communication is outside of normal talkgroup communications and is essentially a private communication between two radio users. Console operators can also place one-way private calls to the radio users. Caution must be used with this feature as it can consume channel availability with just a few users.

- the private call feature is enabled in the user's radio template and system controller
- private call initiation will be limited to essential personnel. Command, high level administrative personnel, radio technicians, radio console operators or those deemed essential by an agency system administrator and approved by Radio Communications Manager

- response only will be allowed on subscriber units
- private call will consume a voice channel for the duration of the conversation
- private calls are not full duplex; only one end can talk at a time
- a low-tier radio cannot initiate a private call; it does not have the feature available
- a mid-tier radio can only place private calls to numbers that are pre-programmed into the radio
- a high-tier radio can place a private call by dialing the number directly via keypad entry
- private calls are recorded by the system
- for the duration of the private call, the users will not be involved in dispatch or talkgroup communications
- the system is not able to restrict the usage of private call, unlike interconnect calls, which can be managed

Operational Context
The private call resource is to be used as a supervisory or system maintenance function. If there is a business need for a radio user to have this ability, it can be granted, but the resource must be closely managed to protect the RF resources of the system. This is also a capability of the dispatch consoles.

Protocol/ Standard
Private call usage shall only be programmed for the users of the system that have a need for the function; the primary purpose of the system is for radio communications. The priority level for private calls is 10; this is defined under the priority section of this document.

Procedure
Radio Communications and the agency radio representatives shall work with the user groups to plan the appropriate private call programming requirements if any, for those users, in order to protect the resources of the system.

Management
Radio Communications is responsible for following this procedure and monitoring the effect and usage of this resource. If negative impact or excessive usage is determined, private call permission can be reconsidered and possibly revoked.

5.16 Emergency Button

Purpose or Objective
Establishes the policy for programming and usage of the emergency button. There is a large variety of users on the radio system with various emergency alarm/notification needs. The various ways the emergency alarm can be configured allows for flexibility of use, however, it is important to plan the use of the feature in such a way that when an emergency button is pushed it is responded to quickly and appropriately.

Radio Communications shall ensure that users are aware of the radio system's emergency signal capabilities, and provide users with a means to properly use this critical emergency feature.

Technical Background

The emergency button feature, if programmed, shall allow a radio user to send an emergency notification by pressing a button on the radio. The notifications audibly and visually alert all dispatch console positions with the talkgroup in their active configuration. Other subscriber radios on the same talkgroup also receive the emergency notification once the 'emergency' radio is keyed and display the radio ID (or alias depending on the model of radio) of the radio generating the emergency.

Emergency calls are also automatically assigned the highest priority available by the system controller and are the first available from the queue if the system is in a busy situation.

Radio template designs must avoid any instance where an emergency is declared, but the user cannot be identified, or the emergency is directed to the wrong dispatcher or agency.

Operational Context

In all trunked radio configurations, the emergency alarm feature is always programmed for the recessed orange button on the top of the portable radio, or the top left feature button on the mobile radio.

An agency can use the emergency button, if they so elect, however the process to receive the emergency notification needs to be documented and contain resolution for the items listed below.

1. No user of the system is provided with emergency signaling capability, unless the user agency provides for 24-hour a day, seven day a week (full time) direct dispatch capability, or has a written agreement with a 24-hour dispatch owner to support this function.
2. Agencies receiving emergency alert activations must have the necessary console hardware/software to receive and display the alert.
3. No dispatcher shall clear an emergency without ascertaining what action is necessary to handle said emergency and taking the appropriate action to do so.

The Department of Emergency Communications Director shall further develop an approved procedure for responding to emergency calls and the proper handling of such calls.

Protocol/ Standard

Use of the emergency button as an emergency signaling option shall be available to any agency on the radio system, subject to certain conditions and provisions.

1. Agencies are not allowed to use this capability of the radio system without prior training provided to all users that have the feature activated in their radio.

2. All agencies implementing the emergency button shall have a plan in place to respond to emergency button activation.
3. It is the individual agency's responsibility to determine how an emergency alarm is answered; which talkgroup(s) are capable of responding to an emergency alarm; and to which talkgroup a specific alarm reverts to.
4. All emergency key response plans must include, at minimum:
   - A central radio monitoring point identifying which radio user pushed the key, the location and nature of the emergency, and the proper agency response.
   - A central monitoring point shall be available during any/all hours that personnel are using the radio system.
   - A policy shall be in place for use of the emergency button by radio users.
   - A response plan shall be in place to assist the radio user in need.
   - In the event the central radio monitoring point is not the same agency as the radio user, an agreement on policy, monitoring, use, and response, shall be in place among the agencies.
5. Any time a user is (temporarily) assigned a radio other than their normal issued equipment, it is essential that their agency dispatch center be aware of the radio identification to cross-reference it to the correct user in the event an emergency button activation occurs.

Management
Agencies desiring to use the emergency key function shall coordinate with agency resources that receive the emergency calls. The receiving agencies shall have an appropriate plan in place and documented as to the process to handle the emergency calls.

5.17 Encryption

Purpose or Objective
Establishes guidelines for the use of encryption on the System.

Technical Background
Encryption is an option on digital radio equipment that must be specially ordered and manually configured. System users may or may not be capable of encryption. AES is the approved standard for encryption. Depending on the level of encryption required, some radios are capable of storing multiple keys for different uses and situations. Motorola's proprietary encryption ADP [may or may not] be used.

Encryption comes in many forms and can be system specific. Care shall be taken to ensure the type of encryption used is compatible with the system and other radios assigned. Radios transmitting in the AES encrypted mode cannot be heard by dispatchers, users with other encryption types, or non-encrypted users. Depending on how encrypted radios are programmed in the system, use of the emergency button may cause the radio to jump to a dispatched and unencrypted talkgroup for handling of the emergency.

Operational Context

ADP encryption is a 40-bit software based form of encryption available only on certain manufacturer's equipment.

AES hardware encryption requires a special module or firmware option to be installed into each unit that provides a Department of Defense grade, 128, 192, or 256 bit encryption scheme.

Protocol/ Standard
Each agency shall determine if encryption will be used on its own talkgroups. System wide talkgroups intended for interoperable communications with outside agencies will not be encrypted at any time.

Procedure
Agencies desiring to utilize encryption shall coordinate with Radio Communications.

Management
The Radio Communications Manager will manage this protocol.

5.18 Bi-Directional Amplifiers (BDA) and Distributed Antenna Systems (DAS)

Purpose or Objective
Establishes guidelines for Bi-Directional Amplifiers (BDA) and Distributed Antenna Systems (DAS) on the System.

Technical Background
The System is designed for county wide radio coverage. However structures such as Music City Center, Bridgestone Arena, correctional facilities, school facilities, etc. may require in-building coverage. BDA and DAS devices are used to bring the radio signal from the outside into parts of building where coverage is not sufficient.

Operational Context
Any Metro agency or department installing a BDA or DAS will coordinate the location, installation, operation, and maintenance of the device with Radio Communications prior to installation. This will include the physical address, location within the facility, manufacturer, model number, system schematics, and the installation and service provider(s).

Protocol/ Standard
When deploying a BDA or DAS, the device must cover the frequency bands of the System, and meet all building and fire codes.

Procedure

Agencies installing a BDA or DAS will contact Radio Communications prior to any building construction or renovations, and will allow Radio Communications unfettered access to the device as necessary.

Management

Radio Communications staff will manage this protocol.

6.0 INTEROPERABILITY STANDARDS

6.1 Interoperable Communication Requirements

Purpose or Objective

Establishes a minimum requirement for interoperable communications resources for all radios utilizing the System.

Technical Background

For the purpose of this document, the terms mutual aid and interoperability will be used interchangeably. The terms channel and frequency will refer to a conventional resource.

The planners of the System recognized the need to make common interoperable talkgroups available to all subscribers primarily for interagency and incident command communications. Therefore, in addition to an agency's normal talkgroups, the 'A Zone' is designed and designated to be programmed into all subscriber radios assigned to the system.

In addition to trunked interoperable talkgroups, the System will also use the conventional nationwide/statewide public-safety channels designated for interoperable communications in each frequency band.

The conventional nationwide/statewide interoperable channels are restricted to non-encrypted plain speech in repeated modes. AES encryption may be used on a 'Tactical' channel in simplex, direct or talk around mode for special units such as SWAT, Drug Task Force, etc., but only when approved by Incident Command or COML.

Operational Context

The 'A Zone' talkgroups/channels are used when there is a significant need to coordinate activities between different agencies and/or personnel assigned to work the event. Examples of these events would be disaster response, fatality investigation, CMA week, HazMat incidents, pursuits, exercises, training, etc. or for Strike Team / Task Force operations. These may be short-term or long-term events.

A patch between any "A Zone" talkgroup and any channel outside of the System is used only if other suitable means for interagency communications are unavailable or if the other available means for coordination of communications are insufficient. Alternatives to an 'A Zone' talkgroup patch may include:

- On-scene use of 8TAC91-94, 8TNMA, 8TNTAC, VTAC11-14, VTNMA, VTNTAC, UTAC41- 43, UTNMA or UTNTAC in repeated or simplex/direct mode.
- Radio to radio cross-band tactical channels, simplex or repeated, via a gateway device such as an ACU-1000, ICRI, B.I.L.L. Box or other gateway device approved by the COML or person acting in the capacity of COML.
- Use of the 'LETSTalk' system where available. 'LETSTalk' utilizes VTNMA, UTNMA & 8TNMA.

Protocol/ Standard

All radios on the System are required to be programmed with the 'A Zone' talkgroups and nationwide/statewide public-safety interoperability channels for each of the frequency bands on which the equipment is capable of operating. Each of these resources shall be designated and labeled by the accepted APCO American National Standards Institute (ANSI) *Standard Channel Nomenclature for the Public Safety Interoperability Channels (http://apcointl.org/standards/apco-standards-for-download.html)* or Tennessee Radio Interoperability Guide (TRIG).

Radio users shall be properly trained in the usage and location in the radio.

Procedure

Normally, an event that requires interagency coordination begins on a main dispatch talkgroup/channel of one or more public safety agencies.

- When it becomes apparent that interagency coordination of law enforcement, fire, Emergency Medical Service (EMS) or other public safety agencies is needed, a dispatch operator or supervisor shall contact the incident commander and coordinate the transition to switch to the assigned talkgroup(s)/channel(s) in the 'A Zone'.
- The specific talkgroup/channel to be used is specified by the designated communications / 9-1-1 center operator or supervisor, incident commander, COML, or designee.
- If the 'A Zone' cannot be used for any reason, or if additional law enforcement interagency intercommunication is required, a console patch between the mutual aid channels and the 'A Zone' talkgroups can be set up by the communications / 9-1-1 center supervisor.

Communications / 9-1-1 center support and the decision to use the console patch is the responsibility of the center supervisor in coordination with response personnel assigned to the incident/event.

Management

Responsibility for monitoring performance and for modifying this procedure is a function of MRAM.

Each communications / 9-1-1 center supervisor is responsible to ensure that there is a procedure for use of a patch between the interoperability channels and the talkgroups in the communications / 9-1-1center.

Public safety communications / 9-1-1 center personnel shall receive initial and continuing training on this procedure and the use of this resource.

6.2 Radio Console Patching of Talkgroups

Purpose or Objective

Establishes procedures for use of (1) a console patch between a System talkgroup and other resources on the dispatch console, (2) a console patch between two System talk groups, (3) a console patch between a System talkgroup and different trunked radio system.

Technical Background

Most public safety communications / 9-1-1 centers have the capability to console patch. Patches can be established between a System talkgroup and other radio console resource. They can be conventional or trunked, analog or digital, but have to be an existing radio resource on the dispatch console. Patches may be established without a radio dispatch console by using a deployable audio gateway, such as an ACU, ICRI or other gateway devices. Approval is required prior to creating a patch. A talkgroup can only be in one patch. A conventional radio resource can only be in one patch. Great care must be used in deciding what talkgroups and other resources can be patched together.
The patch shall be monitored after it is established for continued coordination through Incident Command and/or Communications Unit personnel.

Operational Context

Console Patches should only be used when there is an operational need for communications between personnel using a System talkgroup and another System talkgroup or mutual aid channel. Use must be in compliance with the rules governing the mutual aid frequencies usage. Console patching will only be permitted when approved by communications / 9-1-1 center supervisor if requested by the IC, COMC or COML.

Protocol/ Standard

The communications / 9-1-1 center supervisor is responsible for insuring there are written console patch procedures since each communications / 9-1-1 centers may have different radio resources.

Communications center/9-1-1 operators shall receive initial and continuing training on the use of this procedure.

Procedure

Normally, an event that requires interagency coordination begins on a main dispatch radio channel of one of the communications / 9-1-1 centers. When a request is made by the IC, COMC or COML, the request must be approved by the communications / 9-1-1 center Supervisor.

Before establishing a System patch, check to make sure the radio resource being patched to is not being used for another purpose.

Radio console patches shall be used only if other suitable means for interagency communicating are unavailable or if the other available means for coordination of communications are insufficient.

To minimize interference, console patches to non-System resources will only be allowed for cross-band (VHF to 7/800 MHz or UHF to 7/800 MHz) communications unless approved by the communications / 9-1-1 center Supervisor.

Any time a console patch has been established, someone in the communications center must continually monitor the patch to ensure when problems arise they can be immediately resolved. Monitoring is also required in case additional resources are requested.

Management

The management of the mutual aid channels continues to be the responsibility of the Tennessee Statewide Interoperability Coordinator (SWIC). All users of the System using radio patches to a mutual aid channel shall comply with the Tennessee Radio Interoperability Guide (TRIG).

The Radio Communications Manager is responsible for monitoring performance and revision of this procedure.

6.3 System Talkgroup Patching Via an Audio Gateway Device

Purpose

Establishes the policies for patching a System talkgroup using an on-scene audio gateway.

Technical Background

Agencies / departments in Metro Nashville have deployable audio gateway devices. The gateway may be mounted in a MCV or deployed in a transportable case. Patches can be established between a System talkgroup and other radios connected to the gateway. Patches can be established between conventional or trunked, analog or digital, simplex or repeated radios. A talkgroup can only be in one patch. A conventional radio resource can only be in one patch. Great care must be used in deciding what talkgroups and other resources can be patched together. Not all gateways are capable of patching a trunked radio talkgroup.

Operational Context

Gateway usage must be coordinated and approved by the IC, COMC, COML or person acting as a COML prior to making the gateway operational. An announcement will be made when the gateway is activated. No gateway patches will be established to another agency's dispatch or tactical talkgroups/channels without permission of the agency. Patching to dispatch channels is not recommended. Before deactivation of a gateway, an announcement must be made to ensure no one is utilizing the gateway.

Protocol/ Standard

The Tennessee Radio Interoperability Guide (TRIG) contains the policy / procedures regarding gateway usage.

Procedure

Normally, an event that requires interagency coordination begins on a main dispatch radio talkgroup/channel of a communications / 9-1-1 center. When it becomes apparent that on-scene interagency coordination of personnel from other agencies is needed and participants are on different VHF, UHF, 700 MHz or 800 MHz systems, the use of a gateway may be an effective solution. The decision to use the gateway should be coordinated between communication center supervisor, IC and COML. Once a gateway is activated, a trained gateway operator must be present to monitor the patches and resolve interference or audio issues.

Management

The Radio Communications Manager will be responsible for gateway policy and procedure as found in the TRIG.

6.4 Use of the Nationwide Interoperability Channels

Purpose or Objective

This defines procedures for the use of the nationwide conventional interoperable radio channels for intercommunications between radio users of disparate radio systems and/or different frequency bands.

Operational Background

There are five VHF, four UHF, eight 700MHz, and five 800MHz frequency pairs assigned by the FCC exclusively for interoperable communications between public-safety radio users on different radio systems. One pair in each frequency band is reserved by the FCC as a calling/hailing channel, while the others are reserved for tactical communications, normally used during incident command situations.

These channels follow a nationally recognized naming plan for interoperable radio channels, and are labeled VCALL10, UCALL40, 7CALL70, and 8CALL90 for the calling channels, and VTAC1x, UTAC4x, 7TAC7x, and 8TAC9x for the various tactical channels respectively. These frequencies use analog modulation in a 25 kHz bandwidth repeater mode, or direct radio-to-radio “talk around” mode for on-scene interoperability.

The Metro System has one repeater located at Metro ECC operating on each of the calling channels except 7CALL70, and operational repeaters for the tactical channels on VTAC12, UTAC42, and 8TAC91. The repeaters for 8TAC92, 8TAC93, and 8TAC94 are located at remote tower sites in Davidson County for maximum coverage

There is only one repeater for each of the frequency pairs in Davidson County, so when the decision to utilize one of these resources is made, the repeater located closest to the incident should be used.

Operational Context

These 800 MHz interoperability frequencies can be used for day to day interagency coordination, for urgent or emergency mutual aid situations, and/ or for other purposes where coordination between radio users on separate 800 MHz radio systems must intercommunicate to perform assigned duties.

These channels shall not be used for regular communication between radio users with full access to the Metro radio system except when authorized and assigned by Incident Command.

Recommended Protocol/ Standard

The 8CALL90 and 8TAC91-94 channels are programmed into the '800 Zone' of all subscriber radios on the 800 MHz system unless specified in writing by the agency head of that particular agency.

Outside agencies using the 800 MHz radio system shall have the conventional 8CALL90 and 8TAC91-94 channels included in their fleet maps.

These channels may be used when traveling outside the coverage area of the 800 MHz radio system and are used to communicate with another 800 MHz system with base and/or mobile radios on those channels.

The ECC and OEM Dispatch shall monitor the nationwide calling channels at all times, and they should likewise be monitored nationwide in any other public-safety dispatch center.

Interoperability repeaters can be installed in mobile command posts or other areas as needed.

Recommended Procedure

Normally, events that require interagency coordination begin on a dispatched radio channel of one of the public safety dispatch centers. The dispatch center operator that handles the event initially becomes the responsible dispatch operator and shall provide dispatch service to all personnel in all units participating in the event.

If coordination is required with responders from another radio system, the dispatch center operator or COML shall assign an interoperability channel in the proper frequency band(s) and inform the affected units in their agency to switch to the assigned channel(s). The dispatch center operator or COML that assigned the channel(s) is responsible for all notifications that the resource is being used, and when there is no further need that the resource is released.

When Metro personnel on the 800 MHz system respond to/with personnel using VHF or UHF radio equipment, the dispatch center operator or COML shall either**:**

- Patch a VHF/UHF interoperable channel to an 8TAC91-94 channel, or

- Request that a patch be created at the scene or in another dispatch center with the capability to create the patch.

If interagency coordination is required for a time period longer than a few hours, or if the area where interagency coordination is needed does not have adequate network coverage, a mobile communications unit with on-board repeaters shall be requested to respond to the area of the event operations for better coordination of communications.

If an 800 MHz radio user from outside of Metro Nashville comes into the area and needs assistance, the outside radio user can call for help on the 8CALL90 channel.

Management
Any public-safety radio system user may obtain a license for mobile and portable radio use of the nationwide interoperability radio channels.

Dispatch center managers are responsible for preparing and conducting initial and continuing training for dispatch center operators on the procedures established for use of the nationwide interoperability channels consistent with this procedure.

Responsibility for monitoring the use of and for recommending modifications to this procedure is a function of the MRAM.

6.5 Control Stations Usage on Interoperability Channels

Purpose or Objective
Establishes procedures for the use of control stations for gateway patching.

Operational Background
A control station is a radio that is set up like a portable or mobile, typically with a limited number of talkgroups or conventional radio channels. It can be connected to a radio console or used stand alone.

A control station can function on only one talkgroup or conventional channel at a time.

Use of a control station with a radio console to patch radio system resources can have a wide area impact. This type of patch can be easily accomplished, but may take up multiple trunked radio channels, causing the system to experience busies or possibly create radio interference. Control station usage must comply with parameters listed on the agency's FCC license.

Operational Context
There are a number of uses for control stations including:
- Installed at an agency that does not have a dispatch console to communicate with a repeater or trunked radio system;
- Connected to a console at a communications / 9-1-1 center;

- Installed in Mobile Communications Units/Vehicles;
- Installed at an Incident Communications Center or Command Post.

Protocol/ Standard

Radio control stations are permissible in the following circumstances:

- Connected to a radio console to be used to access the System by non –System user agencies for interoperability purposes;
- Installed in a MCU/MCV;
- Installed temporarily in an Incident Communications Center or Command Post;
- Connected to a radio console to be used to access the System by user agencies for interoperability purposes;
- Used with an audio logger to record transmitted or received audio.

All communications personnel performing the dispatch function shall be trained on the usage and constraints of the control station. They should receive continued training to maintain proficiency and understanding of the procedures.

A Radio Technician, COMT or other authorized person shall be involved in the configuration, installation and testing of control stations, whether a temporary or permanent installation.

Limitations

- Control stations should not be used to patch a System talkgroup to another System talkgroup except when approved by the Communications Center/9-1-1 supervisor.
- Control station antennas must not exceed 20’ in height. If an antenna requires more height than 20’ to access the System or mutual aid repeater, then a FCC license is required.
- No control station antenna may exceed 200’ in height.
- Control stations should use Yagi (directional) antennas when possible.
- Antennas should use the lowest gain possible.
- Control station power should be kept as low as possible.

Procedure

- Any agency wanting to use one or more control stations at the same location is only permitted to use that configuration if the design is compliant with this SOP. The process for obtaining permission is to submit a written request for control station usage to the Radio Communications Manager who will forward it to the Technical Committee for review.
- The request shall describe the location, desired talkgroups, antenna height, power, antenna type, antenna gain and feed line type of each control station.
- The Technical Committee may approve, deny or request modifications to the request.

Management

The Radio Communications Manager will manage this standard.

6.6 Required Monitoring of Interoperability Channels

Purpose or Objective
Establishes procedures for monitoring mutual aid / interoperability channels at Communications Dispatch Centers and in mobiles / hand held radios.

Operational Background
Monitoring of mutual aid channels is imperative for the users needing to contact a dispatch center, Emergency Operations Center (EOC), or other System users. Many channels have been identified to use for interoperability but not all of them need to be monitored nor is it practical to monitor them all. Several statewide mutual aid channels are available. Most local area dispatch centers have Inter-City, VEMS205, VTNMA / UTNMA control stations, or 800MHz Radio System access.

Operational Context
The Department of Emergency Communications, OEM Operations, and Metro's EOC when activated, will monitor specific mutual aid channels or talkgroups. When a unit is calling on one of the monitored channels, the ECC, Metro EOC, or OEM Operations should be monitoring and willing to answer and respond to the call.

Protocol/ Standard
At a minimum, dispatch centers should monitor the following channels or talkgroups if so equipped:

Inter-City
VCALL10
VTNMA
UCALL40
UTNMA
7CALL50
8CALL90

Communications / 9-1-1 centers may monitor local mutual aid channels or additional mutual aid channels.

Procedure
All communications / 9-1-1 center operators shall be trained on the applications and procedures. There shall be on-going training to maintain proficiency and understanding of the procedures.

Management
The ECC Director will manage this section, and will make determination on which mutual aid / interoperability channels should be monitored by communications / 9-1-1 centers.

6.7 Interoperable talkgroups

Purpose or Objective

To establish a dedicated, system-wide, common zone of interoperable talkgroups in all radios assigned to the System for interagency communications when coordination is required between any users on the system, but especially:

- Law enforcement, Fire Suppression, EMS, and OEM
- Metro public-safety agencies, State of Tennessee, and Federal Agencies
- Tennessee Homeland Security District 5 agencies and responders

Technical Background

The planners of the 800 MHz System recognized the need to make common interoperable talkgroups available to all subscribers, but primarily for use by law enforcement and EMS agencies for interagency and incident command communications. Therefore, in addition to an agency's normal talkgroups, interoperable talkgroup zones have been established to facilitate such communications. The 'A Zone' is designed and designated to be programmed into all non-public safety subscriber radios and non-Metro agency radios assigned to the system, and the 'A2 Zone' shall be programmed in all of Metro's public safety radios. Individual talkgroups in these zones reside on both the 'P25 & B System' to ensure that if one part of the System should fail, communication can continue on the remaining channels. All 'A Zone' talkgroups 1 through 10 are not encrypted.

Operational Context

The interoperable talkgroups are only to be used when there is a significant need for communications to coordinate activities between incident commanders of different agencies, and/or personnel assigned to work them, or for special events requiring communications among personnel from multiple agencies.

'A Zone' talkgroups can also be used for short-term high intensity events such as a law enforcement pursuit across county borders, and for long-term extraordinary events like a plane crash or storm disaster.

A patch between any 'A Zone" talkgroup and any channel or frequency outside of the 800 MHz system is used only if other suitable means for interagency communicating are unavailable, or if the other available means for coordination of communications are insufficient. Alternatives to an 'A Zone' patch may include:

- Use of a patch between the 8TAC91-94 channels and VTAC11-14 and/or UTAC41-43
- Radio to radio cross band repeaters between tactical channels at the scene via a gateway device (ACU-1000) at the scene or command site
- Radio console soft patching of a preauthorized VHF or UHF mutual aid or tactical channel to a preauthorized talkgroup on the 800 MHz radio system
- Use of the 'Let's Talk' system

Recommended Protocol/ Standard

The following table shows the layout of the 'A Zone'.

Selector Knob Position	Talkgroup or Channel Name	Primary Usage
1	A1	Unified Command
2	A2	Incident Command
3	A3	Incident Command
4	A4	Tactical
5	A5	Tactical
6	A6	Tactical
7	A7	Tactical
8	A8	Tactical
9	A9	Tactical
10	A10	Tactical
11	A11 8CALL90	National Interoperability - Hailing
12	A12 8TAC91	National Interoperability - Tactical
13	A13 8TAC92	National Interoperability - Tactical
14	A14 8TAC93	National Interoperability - Tactical
15	A15 8TAC94	National Interoperability - Tactical

The following table shows the layout of the 'A2 Zone'.

Selector Knob Position	Talkgroup or Channel Name	Primary Usage
1	A2-1	Unified Command
2	A2-2	Incident Command
3	A2-3	Incident Command
4	A2-4	Tactical
5	A2-5	Tactical
6	A2-6	Tactical
7	A2-7	Tactical
8	A2-8	Tactical
9	A2-9	Tactical
10	A2-10	Tactical
11	A2-11	Metro Command
12	A2-12	Metro Tactical
13	A2-13	Metro Tactical

14	A2-14	Metro Tactical
15	A2-15	Metro Tactical
16	A2-16	Metro Tactical

Recommended Procedure

Normally, an event that requires interagency coordination begins on a main dispatch radio channel of one of the public safety agencies.

- When it becomes apparent that interagency coordination of law enforcement and/or EMS agencies is needed, a dispatch operator or supervisor shall advise the incident commander to switch talkgroups to the 'A Zone'.
- The specific radio channel to be used is specified by the responsible dispatch center operator, incident commander, Communications Unit Leader (COML), or their designee.
- If the 'A Zone' cannot be used for any reason, or if additional law enforcement interagency intercommunication is required, a console patch between the mutual aid channels and/or Interoperable frequencies and the 'A zone' talkgroups can be set up by the dispatch supervisor.

Dispatch center support and the decision to use the console patch is the responsibility of the dispatch center supervisor.

Management

Responsibility for monitoring performance and for modifying this procedure is a function of the Technical Committee of MRAM.

The dispatch center supervisor is responsible to ensure that there is a procedure for use of a patch between the interoperability channels and the 800 talkgroups in the dispatch center.

Dispatch center operators shall receive initial and continuing training on this procedure and the use of this resource.

6.8 Use of the 'LETSTalk' System

Purpose or Objective

This establishes policies for programming and the procedures for use of the Linked Emergency Telecommunications System (LETSTalk) 'LETSTalk' System in Tennessee Homeland Security District 5 (HSD5). The use of any mutual aid or interoperable radio resource requires that the procedures defined in the Tactical Interoperable Communications Plan (TICP) be followed.

Technical Background

A large linked simulcast radio repeater system covering much of the HSD5 geographic area is available for use by all public-safety agencies needing immediate interoperable interagency radio communications between the VHF, UHF, and 800MHz frequency bands.

This system maintains a permanent audio patch between the statewide mutual aid frequencies assigned to each of those frequency bands, is not dependent on any human intervention for its activation, and uses no Metro system resources.

The 'LETSTalk' system is operational in Davidson, Rutherford, Sumner, Williamson, and Wilson counties, and the coverage of this system is considerable.

This patch between mutual aid frequencies can result in radio coverage over an area greater than the service area of the 800 MHz System.

The 'LETSTalk' system is based on analog audio signals, and is therefore subject to the same static and interference issues as the 8TAC90 and 8TACxx channels.

Operational Context

This permanent patch between the VHF, UHF, and 800 MHz mutual aid channels shall only be used when there is an immediate and significant need for radio communications between personnel from different agencies using the separate radio frequency bands

The primary intended purpose of the 'LETSTalk' system is to provide a means of immediate interoperable radio communications between public-safety personnel that are actively engaged in, or are responding to an active police chase, fire, robbery, or other type of incident requiring timely aid or assistance from other cross-border agencies.

These public-safety mutual aid frequencies can also be used for short-term high intensity events, and for long-term extraordinary events.

Recommended Protocol/ Standard

The 'LETSTalk' channel and/or talkgroup will be included in all public-safety agency templates. In order to make this valuable resource quick and easy to locate it is programmed into the agency's primary zone at the very last position. This also corresponds to selector knob position 16 in all radios so equipped, and should make changing to this channel easier to do when in pursuit or running hot.

Normally, an event that requires interagency coordination begins on a main dispatch radio channel of a public safety dispatch center.

When it becomes apparent that immediate interagency coordination of personnel from other county agencies is needed, and participants are on separate VHF, UHF and 800 MHz systems, use of 'LETSTalk' may be required. The decision to use the Lets Talk system should be coordinated between the requesting unit and dispatcher before switching channels.

When an officer, dispatcher, or other responder recognizes the need to utilize 'LETSTalk' to coordinate the actions of separate agencies during an incident, the dispatch supervisor should quickly notify the requested agencies of the activation of 'LETSTalk' and request those agencies responders to use 'LETSTalk' to communicate and coordinate actions with the Metro unit(s)

Management

The use of and the management of the 'LETSTalk' system is the responsibility of the HSD5 Communications Committee and TEMA. This group attained the grant funding, and established the use of that system. All users of the system shall comply with the rules of mutual aid operations.

The dispatch center manager is responsible for ensuring that there is a procedure to notify requested agencies of 'LETSTalk' activation.

Dispatch center operators shall receive initial and continuing training on the use of this procedure.

6.9 Use of the 'MEDTalk' System

Purpose or Objective

This establishes policies for programming and the procedures for use of the 'MEDTalk' System in Tennessee Homeland Security District 5 (HSD5). The use of any mutual aid or interoperable radio resource requires that the procedures defined in the Tactical Interoperable Communications Plan (TICP) be followed.

Technical Background

A large linked simulcast radio repeater system covering much of the HSD5 geographic area is available for use by all Emergency Medical Services (EMS) agencies needing immediate interoperable interagency radio communications between the VHF, UHF, and 800MHz frequency bands.

This system maintains a permanent audio patch between the statewide mutual aid frequencies assigned to each of those frequency bands, is not dependent on any human intervention for its activation, and uses no Metro system resources.

The 'MEDTalk' system is operational in Davidson, Rutherford, Sumner, Williamson, and Wilson counties, and the coverage of this system is considerable.

This patch between mutual aid frequencies can result in radio coverage over an area greater than the service area of the 800 MHz System.

The 'MEDTalk' system is based on analog audio signals, and is therefore subject to the same static and interference issues as the 8TAC90 and 8TACxx channels.

Operational Context

This permanent patch between the VHF, UHF, and 800 MHz medical mutual aid channels shall only be used when there is an immediate and significant need for radio communications between personnel from different agencies using the separate radio frequency bands

The primary intended purpose of the 'MEDTalk' system is to provide a means of immediate interoperable radio communications between EMS personnel that are actively engaged in, or are responding to an active incident requiring timely aid or assistance from other cross-border agencies.

These public-safety mutual aid frequencies can also be used for short-term high intensity events, and for long-term extraordinary events.

Recommended Protocol/ Standard

The 'MEDTalk' channel and/or talkgroup will be included in all Metro Fire and EMS templates. In order to make this valuable resource quick and easy to locate it is programmed into the agency's primary zone at the next to last position. This also corresponds to selector knob position 15 in all radios so equipped, and should make changing to this channel easier to do when running hot.

Normally, an event that requires interagency coordination begins on a main dispatch radio channel of a public safety dispatch center.

When it becomes apparent that immediate interagency coordination of personnel from other county agencies is needed, and participants are on separate VHF, UHF and 800 MHz systems, use of 'MEDTalk' may be required. The decision to use the 'MEDTalk' system should be coordinated between the requesting unit and dispatcher before switching channels.

When an EMT, dispatcher, or other responder recognizes the need to utilize 'MEDTalk' to coordinate the actions of separate agencies during an incident, the dispatch supervisor should quickly notify the requested agencies of the activation of 'MEDTalk' and request those agencies responders to use 'MEDTalk' to communicate and coordinate actions with the Metro unit(s)

Management

The use of and the management of the 'MEDTalk' system is the responsibility of the HSD5 Communications Committee and TEMA. This group attained the grant funding, and established the use of that system. All users of the system shall comply with the rules of mutual aid operations.

The dispatch center manager is responsible for ensuring that there is a procedure to notify requested agencies of 'MEDTalk' activation.

Dispatch center operators shall receive initial and continuing training on the use of this procedure.

7.0 MAINTENANCE RESPONSIBILITIES

7.1 System Maintenance

Purpose or Objective

Defines the system maintenance responsibilities and roles. The maintenance levels for the 800MHz Radio System and its sub-systems shall be set to a standard to protect the overall functionality and integrity of the system for all users. Additional information may be found in the 800MHz Radio System Governance document.

Technical Background
Standards in maintenance protect the integrity of the system and warranties of the sites and equipment. Coordinated maintenance is simplified by having one set of maintenance standards rather than multiple standards.

Improper maintenance poses a risk to the operational functionality of the 800MHz Radio System and its sub-systems and may void equipment warranties.

Operational Context
Each radio tower site and equipment associated with the System is considered "owned" by Metro ITS Radio Communications Division; which is responsible for the maintenance of the sites and equipment. Agreements between ITS and maintenance contractors are at ITS's discretion, but ITS is ultimately responsible for the system.

Maintenance of the system and subsystems is separated into two categories and three severity levels:

- **Categories:** Scheduled (Preventative) Maintenance, and Unscheduled (Corrective or Repair) Maintenance

- **Severity Level Matrix:**

Severity Levels	**Problem Type and Descriptions**
Level - 1	Catastrophic
	Causes loss of functionality of an entire site.
	Simultaneous failure of 50% of the radio channels.
	Failure of all console positions at any communications center.
	Loss of the ability to report backbone alarms or any alarms which might indicate a catastrophic failure.
	Loss of multi-site controls or networking.
	Loss of simulcast capabilities.
	Loss of Trunking capabilities.
Level - 2	Non-Catastrophic: A non-catastrophic failure is not repaired within the response time specified herein for the operational system.
	All Fixed equipment failures that are not categorized as Severity Level - 1 failure.
Level - 3	Preventative Maintenance Activities

Recommended Procedure

Any widespread maintenance issues that affect multiple agencies shall be discussed and resolved at MRAM.

For day-to-day maintenance, the ITS Radio Communications Division or its contract vendor shall maintain the equipment.

For emergency and urgent repairs, Radio Communications may request and expect cooperation from support resources (e.g. - support staff and/or parts) from other agencies to restore equipment/systems to normal operation.

Repair of any equipment not normally maintained by Radio Communications requires the notification and consent of the owning agency.

Radio Communications and/or their contracted service providers are responsible for:

- FAA registrations, FCC ASR registrations and FCC licenses, ensuring that equipment is properly licensed and copies of the licenses are posted at the sites as required by regulations.
- Maintaining equipment within the limits of Metro Nashville's FCC licenses.
- Notifying the responsible personnel of equipment and location issues that require attention.
- Managing the inventory of the radio subscriber and infrastructure equipment.
- Ensuring that equipment at the tower sites that is not part of the radio system inventory shall be clearly labeled to indicate agency ownership.
- Routine equipment maintenance logs are kept at the sites.
- Maintaining current copies of all as-built documentation at each site and at the Radio Communications Field Services office. Radio Communications Field Services office is responsible for ensuring the accuracy of all as-built data related to the infrastructure equipment and any changes shall be immediately documented. Radio Communications shall distribute the updated information as required.
- Coordinating, implementing and/or overseeing configuration changes affecting the system infrastructure.
- Any work being scheduled affecting the system and/or sub-systems performance and reasonable notification to the system's users of same.
- Ensuring all technicians assigned to work on system equipment have successfully completed appropriate training on the equipment. Training requirements are referenced in the training section of the standards manual.
- Following a preventive maintenance plan as defined in the preventative maintenance section of the manufacturers' manuals.
- Maintaining a list of the qualifications and contact information of technical staff in the event of an emergency, found in the Business Continuity and Disaster Recovery (BCDR) Plan.
- Maintaining a list of the available spare parts/equipment pertaining to the system and sub-systems. All infrastructure spares, after returning from the repair center, shall be

re-installed into the same location they were removed from and verified for correct operation prior to closing the repair case.
- Ensuring any equipment upgrades or changes affecting normal operations of the system are adequately discussed and approved by the Technical Committee.
- Determining how critical an equipment failure is operationally, determining the appropriate action, and escalating or de-escalating the repair process as needed.

Management
Radio Communications is responsible for managing the maintenance of the radio system equipment and sites and managing the repair responsibilities in emergency situations.

7.2 Maintenance Notifications / Contact Information

Purpose or Objective
Defines the procedures and processes for maintaining the internal and external contact information for staff supporting the System and for the secure distribution of the contact information.

Technical Background
Having the contact information readily available to the system support staff facilitates:
- General purpose day-to-day communications
- Source information for distribution lists
- Notification for equipment / location issues
- Contacting support staff in the event of a system failure, after-hours service calls, power availability and quality, or disaster recovery
- Having a current list of vendor support contacts
- Facilitating the information electronically / centrally eliminates duplication of effort

The contact information shall be kept up to date and available to the support staff of the System. This information is classified as ‘Restricted Information”.

Operational Context
Radio Communications will maintain current contact information of administrative, technical, support staff and vendors. Radio Communications will develop an on-call procedure for system or site issues.
The contact information shall contain:
- Internal support staff, radio communication technicians, radio communications supervisors, radio system analysts, administrative staff, etc.
- External support staff, contractors, subcontractors, generator maintenance, equipment providers, electrical contractors, and telecommunications providers responsible for site connectivity etc.
- Providers of utilities, fuel, tower and site lighting, site security equipment, fencing, equipment shelters, etc. Includes any responsibility for right-of-way to access sites in the event road conditions or trees down impede access during emergencies]
- Building security contacts

Radio Communications staff is responsible for the accuracy of the contact information. The contact information is kept on the Radio Communications storage server and is available to appropriate staff.

Protocol/Standard

Radio Communications staff shall utilize dedicated data storage servers to store emergency contacts and documents related to site disaster planning and recovery. The contact list is shared between all agencies to store all pertinent contact and disaster recovery information.

Procedure

Radio Communications shall maintain all contact information of support staff in a database stored on a on an "off-site" backed-up server dedicated to Radio Communications on the Metro in the event of a disaster. The resource shall be accessible to appropriate staff.
The contact information to be saved includes such things as:

- Name
- Agency
- Functional role
- Work address
- Contact phone numbers "work, home, pager, cell" at the support person's discretion.
- Email addresses

This information shall be verified bi-annually by Radio Communications staff. Any changes to contact information shall be updated immediately upon notification.

Management

Radio Communications is responsible for this process, through coordination with equipment and service providers and vendors.

The contact database is updated as changes are received, and audited / reviewed for accuracy and updates on an annual basis.

7.3 Maintenance / Repair Notifications

Purpose or Objective

Defines the procedure for notifications of scheduled and unanticipated maintenance activities having an impact on normal system operations, system interruptions and outages.

It is the policy of MRAM to provide guidelines for radio user notifications by Radio Communications for any maintenance actions having a potential for system interruptions.

Technical Background

Typically, equipment functionality can change when hardware and software configuration alterations or other maintenance activities are performed. Advanced notification of planned maintenance activities that impact the normal operation of the system allows user agencies

and subscribers to make preparations as needed. Notification will also be made to user agencies when a catastrophic failure happens.

If the notification process is difficult and lengthy, it can become a barrier to making notification to user agencies.

Failure to make proper notification to user agencies can result in unneeded confusion, disruption or loss of public safety communications, and possible compromise of any special operations communications.

Operational Context

Affected agencies shall be notified of maintenance activities that impact their subscribers on the system. Agency notification of radio maintenance activities to their individual subscribers is at the discretion of the user agency's designated representative.

Protocol/ Standard

Radio Communications is responsible for monitoring the system on a 24-hour basis, whether it is by on site personnel or by an automated electronic monitoring and notification process. Maintenance activities, planned or unplanned, that could impact the subscribers usage of the system requires notification to the affected agency's radio representatives.

In the event of planned maintenance, all efforts should be made to conduct this type of activity during off-peak hours where radio utilization is as low as possible. If an emergency or high priority incident is in progress at the time of scheduled maintenance, it may be necessary to reschedule or delay the maintenance until the situation has stabilized and can be safety moved to alternate talkgroups or channels.

Procedure

A reasonable advance notice shall precede planned maintenance activities that affect the agencies of the system. The notification methods shall be by phone, e-mail, radio, or any combination of the same. The notification will consist of:

- The type of planned maintenance activity
- When the maintenance will be conducted
- The amount of time anticipated to complete the activity
- The anticipated impact to the system and subsystems

If a known activity has a significant operational impact upon any specific agency, a confirmation of receipt of notification shall be obtained. It is the responsibility of Radio Communications to ensure that all affected users are notified well in advance of any such operations. Whenever possible, these operations shall be scheduled when the normal radio traffic is slowest.

Prior to commencing the maintenance operation, personnel from Radio Communications shall contact each affected dispatch center's supervisor for a last minute situational briefing. At that time Radio Communications personnel shall, as determined by the briefings, make the GO / NO-GO decision.

Once maintenance operations begin, if dispatch operations recognize a need to terminate the operation, or if unexpected problems occur, a communications supervisor must call the lead technician working the maintenance operation to inform the technicians of the situation.

Unanticipated maintenance or equipment failures affect the agencies on the system and require notification to the affected agency's radio representative.
Upon notification of an equipment outage, Radio Communications technical staff is expected to:

- Determine the impact of the impairment to the operation of the system. A minor failure is something that either does not affect or minimally affects user functionality. A major alarm is something that seriously affects or risks user functionality of the system.
- Determine if there are internal or external factors that alter the priority of system impairment, such as weather, subscriber loading, unique public safety activities or impending events, etc.
- Determine if manual intervention is required. A serious failure requires initiating repair processes regardless of the time of day. Minor failures can wait until normal business hours or other convenient time before repair. The determination is at the discretion of Radio Communications, and shall be based on internal system functionality and external subscriber needs.
- Determine if additional external resources are required.

The Notification process for maintenance activities is defined in the "Maintenance/Repair Notifications" Section 7.3 of this section.

Once the operation or repairs are complete, Radio Communications personnel shall contact the dispatch supervisors for an update and user feedback.

When requested by MRAM or the Technical Committee, the details of recovery processes may be reviewed for improvements.

Management
Each agency's radio representatives are responsible for notifications within their respective agencies.

7.4 System Coverage

Purpose or Objective
Establishes the requirements for regular outdoor testing and verification of System signal quality and coverage.

Technical Background

Signal coverage of the system fluctuates constantly and is influenced by many conditions including but not limited to:

- Terrain
- Weather
- Vegetation
- Building Construction
- Equipment Condition
- Location

Regular sampling of signal quality and strength at pre-designated locations will help to confirm adequate coverage, or if a problem might have developed in certain locations due to changes in one of the above conditions

Operational Context

Periodic coverage testing is a critical component of system operation and maintenance, and will continue toward identifying and mitigating any signal coverage issues, including any potential effects of new building construction and development.

Protocol/ Standard

Radio Communications staff will perform a semi-annual comprehensive signal coverage test to evaluate the System's signal strength and quality across the service area. The locations and number of individual test points shall be based on the area's building density and known areas of poor coverage.

The results of each test will be compared to previous results and monitored for signal degradation. Test results will be stored on a shared data server for historical comparisons.

Management

The Radio Communications Manager oversees the process, evaluates the results, develops remediation strategies, and reports significant findings to MRAM.

7.5 Repair Parts Inventory

Purpose or Objective

Establishes an inventory control procedure for infrastructure and subscriber repair parts.

It is the policy of MRAM to ensure that planning is in place and available resources identified to expedite the recovery of the System and related components in the case of disaster, catastrophic failure or other major incident that affects operations of the system.

Operational Context

Radio Communications will maintain a vendor recommended inventory of spare parts for regular repairs to the System and subscriber radios.

Protocol/ Standard

The spare parts inventory for infrastructure shall be kept at the Metro ECC offices. Parts for subscriber units shall be kept in the dedicated stockroom at MSE. An 'Advance Replacement' agreement with the system vendor shall be utilized to ensure that as parts are used for infrastructure repairs, those parts are immediately replaced with working units to avoid delays in returning defective equipment to service. All parts will be tracked

Management

The Radio Communications Manager maintains and manages the plan

7.6 Disaster Recovery

Purpose or Objective

Establishes the minimum requirements for a system disaster recovery plan.

It is the policy of MRAM to ensure that planning is in place and resources identified and available to expedite the recovery of the System and related components in the case of disaster, catastrophic failure or other major incident that affects operations of the system.

Operational Context

Radio Communications personnel with the assistance and guidance of ITS, OEM, and Emergency Support Function (ESF) 2 will maintain a comprehensive plan for restoration of the System during times of disaster. If the Metro Emergency Operations Center is activated, ESF 2 must be notified of the system problem so that it can be logged into WebEOC.

Protocol/ Standard

The plan is maintained by the Radio Communications Manager. The Disaster Recovery Plan should contain contact information for all Metro, vendor, and contracted support personnel, and basic recovery processes. The Plan should address different types of training for different levels of users so they will be familiar with the plan, aware of their roles, their responsibilities, and course of action in the event of a catastrophic loss of communications. The Plan should contain alternative communications methods to be used during the system recovery.

Management

Radio Communications Manager maintains and manages the plan; MRAM is responsible for updates.

8.0 SITE AND SYSTEM SECURITY

8.1 Site Security

Purpose or Objective

Establishes the minimum requirement to provide site security and protect the integrity of the System's radio towers, equipment shelters and equipment.

Technical Background

Security measures have the overall benefit of protecting the functionality, integrity and operation of the system. Details of specific security measures cannot be placed within a public document; otherwise measures used in monitoring and maintaining security are compromised.

Operational Context

The physical security of equipment, facilities, and structures making up the core of the radio system infrastructure is paramount to the reliability and availability of communications carried on the system. Each site is within a fenced, gated and locked compound, with shelter entry monitored and reported to a central monitoring point. A remote controlled camera system is installed at each site and is monitored for any unauthorized entry or security concerns.

Each site must have an address issued by the local 911 Emergency Communications District.

Protocol/ Standard

Access to the sites is tightly controlled and entry to those sites is granted only to those personnel with proper authorization from Radio Communications. All personnel requiring unaccompanied site access must submit a signed Tower Site Access Request/Agreement, have passed a comprehensive background check, and be on the list of personnel with approved access prior to access. Personnel without proper background clearance must be accompanied by Radio Communications or approved Metro staff. Entry alarms for the remote sites are sent immediately to the Radio Communications technical support staff and the ITS Help Desk, as well as other site alarms. A copy of the Tower Site Access Request/Agreement is found in Appendix #4.

Procedure

Notification to the ITS Help Desk and Radio Communications technical support staff is required of all agencies and vendors prior to gaining site access. Any person requiring access to the tower sites for any reason shall have full clearance from Radio Communications or be accompanied and monitored by Radio Communications personnel while there. Law enforcement personnel will be immediately notified and dispatched to any site with unexpected or unexplained alarms or unidentified personnel viewed remotely from the camera systems.

Any agency or vendor with access to any tower site or equipment location shall make immediate notification to the Radio Communications Manager of urgent issues such as discharged employees or cancelled contracts.

When a site has been vandalized or broken into, the jurisdictional law enforcement agency should be notified. The person who discovers the event has the responsibility to preserve the crime scene and not contaminate it. He/she should have the ECC log the time when the event was discovered and any other pertinent information relating to the site/scene. Then the ECC should then notify Metro Police and Radio Communications. Other agencies may be notified if they own equipment at the site. Radio Communications will notify all affected agencies as soon as possible.

When the site is off the air due to a crime, the technician should refrain from making entry unless permission has been given by the Radio Communications Manager due to extreme circumstances taking place that requires coverage from the site.

If a radio technician should arrive at a site and an unauthorized vehicle or person is on the property, they should back off and call 911. The technician should give the 911 call-taker the street address and advise them of the situation. The technician should also notify his/her supervisor. At no time should the technician put themselves at risk of harm.

If a technician has to respond to a vandalized remote site after normal business hours, it is recommend for safety reason that a minimum of two persons respond to the site. A Metro Officer may be requested to go to the site with the technician.

Management
The Radio Communications Manager is responsible for managing this procedure.

8.2 Network Operational Security

Purpose or Objective
Establishes the specific security measures for system and subsystem equipment and to define site security policy.

Technical Background
Security measures have the overall benefit of protecting the functionality, integrity and operation of the system. Details of specific security measures cannot be placed within a public document; otherwise measures used in monitoring and maintaining security are compromised.

Operational Context
Equipment and site security is a continual process.

Protocol/ Standard

All items identified as 'Restricted Information' will be maintained in secure areas within the control of Radio Communications and is not available outside of Radio Communications except by formal written request.

Technical information that can compromise system security is considered 'Restricted Information'.

The System's network is protected from other data networks by isolation or by using a properly configured firewall having the approval of both Metro ITS and the system manufacturer.

All remote access points to the system are kept secure and are coordinated with the Radio Communications Manager.

Passwords protect the system and subsystem equipment for the purpose of preventing unauthorized access to equipment. The Radio Communications Manager issues the passwords.

User login accounts are protected with passwords providing an appropriate level of protection. If a password is suspected of being compromised, it is immediately updated or the user account will be disabled pending resolution.

External devices (computers, modems, routers, data storage, etc.) are not connected to the system network, computers, or consoles without the approval of the Radio Communications Manager and have the proper anti-virus software. All external devices connected to the system must be supplied and supported by Metro ITS, the technician's IT department, or the system vendor.

At no time will any personally owned device be connected to any port or connector on the System

It is recommended that computers used for programming or maintenance not be connected to the internet to help reduce possibility of virus infection.

Procedure

All agencies, contractors, and personnel that require access to MRAM controlled sites must provide signed copies of the Tower Site Access Request/Agreement, and each person that will access the sites must pass a comprehensive background check before unaccompanied access is allowed. The agreement is found in Appendix 4.

System documentation is classified 'Restricted Information'.

Management

The Radio Communications Manager is responsible for the network, equipment, and site security of the system.

8.3 Software, Firmware and Document Security

Purpose or Objective
Establishes the minimum security measures and procedures to protect the integrity of the System's software and programming.

Technical Background
The documentation, service and technical manuals, databases, spreadsheets and software of the System contain critical operational and technical information that could compromise the system if obtained by unauthorized personnel and is classified as 'Restricted Information' in accordance with Metro Nashville's Information Classification Policy.

Operational Context
The documentation and software of the system changes as the system evolves. Those changes and revisions must be documented and maintained in a central location for quick and easy access for the technical support staff.

Protocol/ Standard
In the best interest of public safety, all documentation, service and technical manuals, databases, spreadsheets and software of the System are considered 'Restricted Information' in accordance with Metro Nashville's Information Classification Policy.

Software relating to the programming of any System component shall only be installed on authorized government owned computers or ITS authorized contractors' computers.

Procedure
All items identified as 'Restricted Information' will be maintained in secure areas within the control of the Radio Communications Manager. These items will only be shared with those who require knowledge of it for operational purposes. This information is not available to anyone outside of Metro. An exception may be made with a formal written request and approval from MRAM. This information is not to be released to any personnel who do not have a legitimate and appropriate need for it.

Management
The Radio Communications Manager is responsible for managing this procedure.

9.0 APPENDIX

9.1 Mayor Briley's Executive Order #19

THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

DAVID BRILEY, MAYOR

Subject: Emergency Radio Management Committee

I, David Briley, Mayor of the Metropolitan Government of Nashville and Davidson County, by virtue of the power and authority vested in me, do hereby find, direct and order the following:

I. The Metropolitan Government and the Nashville Electric Service (N.E.S.) embarked on a project to purchase, construct and operate an 800 MHZ trunked radio system (the "System") to improve emergency dispatch and response throughout Davidson County; and,

II. Even though the digital radio technology in the System provides greater radio bandwidth, the licenses issued to the Metropolitan Government by the Federal Communications Commission provide only a limited radio bandwidth to the Metropolitan Government; and,

III. In order to utilize the System to its fullest potential and preserve its availability for emergency use, the Metropolitan Government must efficiently manage and control access to the System; and,

IV. In December, 1997, the Metropolitan Government and Nashville Electric Service entered into a Memorandum of Understanding that included a provision for a joint committee to manage the access to and operation of the 800 MHZ trunked radio system.

1. There is a Metropolitan Government Emergency Radio Management Committee for the Metropolitan Government of Nashville and Davidson County.

2. The membership of the Metropolitan Government Emergency Radio Management Committee shall be as follows:
a. The Director of Information Technology Services, or his or her designee;
b. A representative selected by N.E.S.;
c. The Chief of Police, or his or her designee;
d. The Fire Chief, or his or her designee;
e. The Purchasing Agent, or his or her designee;
f. The Director of General Services, or his or her designee;
g. The Nashville Sheriff, or his or her designee;
h. The Director of Public Works, or his or her designee;
i. The Director of Water Services, or his or her designee;
j. The Director of Parks & Recreation, or his or her designee;

k. The Director of the Office of Emergency management, or his or her designee;
l. The Director of the Department of Emergency Communications, or his or her designee;

3. The Police Department, Fire Department, Department of Emergency Communications and N.E.S. are expected to be the major users of the System. Information Technology Services will have the major operating and maintenance responsibilities for the System. Therefore, these five (5) agencies will be the lead agencies on the Committee and shall have two (2) votes each. The other named Metro agencies represented on the Committee shall have one (1) vote each. Non-Metro agencies participating on the System will not have a vote but are encouraged to send a representative to attend the committee meetings.

4. The Director of Information Technology Services, or his or her designee, shall serve as Chair. The Committee shall select a Vice Chairman from another agency who will serve for a term of one (1) year. The Committee shall adopt any additional rules for internal governance it deems necessary. The staff services to the Committee will be provided by the Department of Information Technology Services.

5. The mission of the Metropolitan Government Emergency Management Committee is as follows:
a. Develop and implement guidelines for the allocation of effective and efficient use of the System, including the loading and development for all users.
b. Review and disseminate the annual recommendations provided by the Director of Finance that relate to a fair and proportionate rate structure by which to assess each user for the recovery of maintenance and operating costs of the System.
c. Provide long-range planning for the continued operation of the System.
d. Consider, review, make recommendations for, and resolve all requests for system access or connection.

ORDERED, EFFECTIVE AND ISSUED:

David Briley
Metropolitan County Mayor

Date:

9.2 Contacting Radio Communications

Use one of the following methods to contact Metro Radio Communications staff for access, radio issuance, equipment programming, service, and lost radio notification:

- During normal working hours, Monday – Friday, 7:30AM – 4:00PM - **(615) 862-5111**
- Outside of normal working hours, or to make emergency service requests contact the ITS Help Desk at **(615) 862-6222**

Phone Numbers:

MSE Shop Main Line	(615) 862-5111
MSE Shop Fax	(615) 862-5123
Field Service Office	(615) 862-8561
Field Service Fax	(615) 880-3494
ITS Help Desk	(615) 862-6222

Physical Addresses:

Radio Issuance and Programming Services
Radio Communications Shop
Metro Southeast
1417 Murfreesboro Pike
Nashville, TN 37217

Field Services and System Operations
Radio Communications Field Office
Metro Emergency Communications Center
2060 15th Avenue South
Nashville, TN 37212

Mailing Address:
Metro Radio Communications
P.O. Box 196300
Nashville, TN 37219-6300

9.3 System Access Request Form

This is an abbreviated sample of the actual request form.
An official form should be requested from MRC for completion.

Name of Agency, Department, or Organization:
Primary Address:
Primary contact information:
Primary Contact Person:
Telephone Number:
Primary Email address
Secondary Contact Person:
Telephone Number:
Secondary Email Address:

How many units require access?

Portables _____ Mobiles _____ Control Points _____ Consoles _____

Please provide answers to the following questions as needed for your specific request.

☐ Are you requesting INTEROPERABILITY with the Metropolitan Government?
Please explain why

☐ Do you require User Level System Access, i.e., your own Talk group(s)?
If so, how many, and why?

☐ Do you require System Connectivity for equipment (Dispatch Consoles, Repeater Site)?
If so, please explain.

If you require interoperability with other agencies please check the associated box and provide your justifications for this access for each group.

☐ Nashville Electric Service
☐ Metro Fire/EMS
☐ Metro Police
☐ Metro Office of Emergency Management
☐ Metro Park Police
☐ Unified Command for Public Safety Agencies
☐ Board of Education
☐ Codes Department
☐ Juvenile Court
☐ Public Works
☐ Sheriffs' Office
☐ City of Belle Meade Police
☐ City of Berry Hill Police
☐ City of LaVergne

☐ City of Mt. Juliet
☐ City of Goodlettsville
☐ Vanderbilt University Police
☐ Other Agency Not Listed

9.4 Tower Site Access Request/Agreement

Metro Radio Communications
Tower Site Access Request Form

This form must be completed by all agencies and vendors requiring access to Metro Radio Communications tower sites.

Name: _____ Date: _____/_____/_____

Company: _____

Department: _____

My signature on the line below indicates that I have read and completely understand the following, and will abide by these rules regarding access to any Metro Radio Communications tower site.

1. Access to the sites is tightly controlled and entry to those sites is granted only to those personnel with proper authorization from MRC. Entry alarms at the remote sites immediately alert MRC personnel of any intrusions.

2. A tower site access list shall be maintained by MRC, and be kept up to date, including vendor support staff. The site access list will be closely monitored. A person will be denied unsupervised access to any site if that person is not identified on the access list.

3. Vendors must ensure their personnel are properly authorized and are on the current authorization list prior to dispatching someone to work at a tower site. An unauthorized technician will only be allowed access to a site when accompanied and supervised by one with the proper authorization. All unauthorized personnel at any tower site will be under the supervision of MRC authorized staff.

4. All personnel must pass a background check administered by Metro Police before unsupervised access is granted to any Metro Radio Communications facility.

5. Site access shall not be unreasonably denied to Metro agency support staff, which are responsible for maintaining their agency's equipment located at that site as long as they have passed the background check.

6. External devices (computers, modems, routers, etc…) are not connected to the system network without the approval of MRC.

7. Site access is not unreasonably denied to outside agency support staff, but is closely monitored and can require escort by MRC staff. Outside agencies requiring site access are required to coordinate all site visits with MRC staff during normal working hours. After-hours access is tightly controlled and is generally discouraged unless it is an emergency.

8. Access to any site without first contacting Metro ITS Help Desk and Radio Communications is prohibited, and shall result in disciplinary action against the offending agency and can result in removal of the agency's equipment and total site restriction, or loss of contract privileges.

9. Any agency or vendor with access to any tower site or equipment location shall make immediate notification to Radio Communications of urgent issues such as discharged employees or cancelled contracts.

10. The physical security of equipment and structures making up the core of the radio system infrastructure is paramount to the reliability and availability of communications carried on the system. Each site is within a fenced, gated and locked compound, with shelter entry monitored and reported to a central monitoring point through the MOSCAD alarm and control system. A remote controlled camera system is installed at each site.

11. Any person requiring access to the tower sites for any reason shall have full clearance from MRC, or be accompanied and monitored by a MRC authorized technician while there.

12. MRC reserves the right to dispatch law enforcement personnel at any time to ensure security of the tower sites.

I further signify that I understand and accept the risks involved with the possible exposure to radio frequency emissions, and all other personal hazards involved within the confines of the site, and I hereby release Metro Nashville Government, its employees and officials from any and all liability from access to any tower site or structure, and any injuries that might occur from the same.

Signature: _____

Date: _____/_____/_____

9.5 Radio Equipment Damage/Loss Report Form

Radio Equipment Damage/Loss Report

All agencies and users are required to report any damage, loss, or theft of Metro owned radio communications equipment as soon as possible, and submit a completed copy of this form within 48 hours of the incident to Metro Radio Communications. If the equipment was lost or stolen, a police report is also required.

Damage / Loss / Theft - Reported By	
Employee Name:	Employee Number:
Position/Title:	Department:
Phone:	Email:

Incident Information	
Incident Date: ___/___/___	Time of Incident:
Reported on: ___/___/___	Time Reported:
Supervisor:	

Equipment Information	
List of Equipment Damaged / Lost / Stolen (Please Specify)	
Equipment Identification Number(s)	Model: Serial Number: Asset Tag:
Equipment Location at Time of Damage / Loss	

How Was the Equipment Damaged / Lost / Stolen? (Complete Description)	
Description of Damage to Equipment	
Estimated Cost of Repair / Replacement	
Person Responsible for Equipment	

Police Report Information	
Police File/Report #:	Officer:
Precinct:	Phone #:
Email:	

Report Submitted By:

Name: _____ Signature: _____

Date: _____

Received by Metro Radio Communications:

Name: _____ Signature: _____

Date: _____

Work Order #: _____
Estimated Replacement Cost: $_____

Notifications:

Division Manager: _____ Date & Time: _____
Asst. Director: _____ Date & Time: _____
Department Rep: _____ Date & Time: _____

9.6 Glossary – Definitions and Acronyms

Item/Acronym	Definition
700MHz	For Public Safety LMR, digital P25 voice radio channels between 769/775 MHz and 799/805 MHz. Channels have 30 MHz seperation between Tx & Rx when repeated. FCC designated low power channels can be used analog voice.
7CALL / 7TAC	Nationwide 700 MHz Calling and Tactical channels
800MHz	For Public Safety LMR, analog or digital voice or data radio channels between 806/816 and 851/860 MHz. Channels have 45 MHz seperation between Tx & Rx when repeated.
8CALL / 8TAC	Nationwide 800 MHz Calling and Tactical channels
ACU-1000	An audio gateway device capable of connecting disparate radio systems, channels, or talkgroups together during on-scene operations, similar to a console patch between talkgroups
AES	Advanced Encryption Standard
Alias	A common alphanumeric name used to identify a radio, talkgroup, site, etc. rather than referencing the assigned 6 digit ID number
ANSI	American National Standards Institute
APCO	Association of Public-Safety Communications Officials
APCO P25	A public-safety digital radio standard
ASK	Advanced System Key
BCDR	Business Continuity and Disaster Recovery
BDA	Bi-Directional Amplifier, relays radio signals into and out of a building
BER	Bit Error Rate
Channel	A pair of frequencies, transmit and receive, that are used for a single communications path
Channel Bank	A device that combines multiple data and/or audio inputs into TDMA format so that it can be transmitted over microwave or T1 circuit and shared between transmitter sites
COMC	Communications Coordinator
COML	Communications Unit Leader
COMT	Incident Communications Technician
Console Patching	Ability to connect channels via dispatch consoles
Consolette	A mobile radio mounted into a case with power supply and converted for desk-top use
Control Station	An installed radio unit, sometimes a mobile radio, normally found at a desk or common work area indoors or directly connected to a console or other fixed transmitting location

Item/Acronym	Definition
DAS	Distributed Antenna System, relays radio signals into and out of a building
DCSO	Davidson County Sheriff's Office
Digial radio	Digital radios turns sound (by signal processing) into patterns of digits (numbers) rather than the radio waves which are used for analog transmissions.
Dispatch Console	A fixed radio operator position with multiple radio resources and features that can access any subset of talkgroups and/or conventional channels
ECC	Emergency Communications Center
EIA	Electronic Industry Alliance
EMS	Emergency Medical Services
EOC	Emergency Operations Center
ESF	Emergency Support Function
FAA	Federal Aviation Administration
FCC	Federal Communication Commission
Fixed	Radio equipment that is installed at a radio site or dispatch center
Fleetmap	The master spreadsheet plan of the talkgroups, zones, Failsoft assignments, alias information and other pertinent system and radio programming
FM	Frequency Modulation
Gateway	A device that allows two or more radio or voice devices to be connected together
IAP	Incident Action Plan
IC	Incident Command
ICALL	Calling Channel for ITAC
ICC	Incident Communications Center
ICP	Incident Command Post
ICRI	Incident Commanders Radio Interoperability, a gateway device
ICS	Incident Command System
ICS 205	Incident Radio Communications Plan
ICS 217	Communications Resource Availability Worksheet
ID	Identification
INCM	Incident Communications Center Manager
Infrastructure	All of the fixed electrical and mechanical equipment, towers and building structures, generators, transmitters, controllers, antennas, microwave and ancillary equipment that comprise the operational backbone of the radio system
Inter-agency	Located or occurring between two or more agencies
Interoperability	The ability of Public Safety responders to share information via voice and data communications systems on demand, in real time, when needed, and as authorized.

Item/Acronym	Definition
Interoperable	Ability of a system to use the parts or equipment of another system
ITAC	Conventional mutual aid channel 800 Mhz
ITS	Information Technology Services
LDRPS	Living Disaster Recovery Program System
LMR	Land Mobile Radio
Logging	The act of recording radio conversations for replay as required
MCC	Mobile Communicaiton Center
MCU	Mobile Communications Unit
MCV	Mobile Communications Vehicle
MFD	Metro Fire Department
MHz	Abbreviation for megahertz. 5 MHz = 5,000,000 Hz or 5,000 kHz. A unit of measure for the number of times a frequency makes one complete cycle in one second
Mission Critical	For mission critical applications, users have an expectation of "immediate" communication with their dispatch or command center and little to no end-to-end audio delays.
MNPD	Metro Nashville Police Department
Mobile Radio	A vehicular mounted radio with an power source and antenna
MRAM	Metro Emergency Radio Management Committee
MRC	Metro Radio Communications
Mutual Aid	Personnel, equipment, or services provided to another jurisdiction
NECP	National Emergency Communications Plan
NGOs	Non-Governmental Organizations
NIMS	National Incident Management System
OTAP	Over the Air Programming
OTAR	Over the Air Rekeying
P25	A suite of standards for digital radio communications for use by federal, state and local public safety agencies in North America to enable them to communicate with different vendor radio systems using a common platform
Patch	Electrically connecting two or more radio channels or talkgroups so that those users of those separate resources are able to communicate with each other
POC	Point of Contact
Portable	A lightweight, completely self-contained radio unit usually worn on user's belt
Public Safety	An agency, department, or individual directly involved with the health, safety, and/or security of the public including, but not limited to police, fire, emergency management, and medical personnel and responders

Item/Acronym	Definition
Public Service	An agency, department, or individual involved with providing non-emergency type services to the public including, but not limited to utilities, transportation, education, and other governmental services, supporting public safety
RADO	Radio Operator
RF	Radio Frequency
SCIP	Statewide Communications Interoperability Plan
SEOC	State Emergency Operations Center
Simplex	Radio to radio communications on one frequency. Also called Direct
Simulcast	A type of radio communications in which voice communications are transmitted from multiple radio sites and can be received simultaneously by field units to provide wide area coverage
Site	The physical location of an antenna tower, equipment shelter and radio system infrastructure equipment
SOP	Standard Operating Procedure
SOW	Site on Wheels
Subscriber Unit	A mobile, hand held or control station radio used on a trunked radio system
SWIC	Statewide Interoperability Coordinator
TAC	Tactical on scene operation
TACN	Tennessee Advanced Communications Network
Talk Around	Radio to Radio communications on one frequency, usually the same frequency on which a repeater transmits. Simular to Direct or Simplex
Talkgroup	Term ususally used with trunked radio systems. A talkgroup is a predefined list of radios/users assigned a unique ID which allows them to communicate with each other over the trunked radio system.
Talkgroup Alias	Abbreviated naming of the talkgroup to fit within the 8 or 14 character radio display
Talkgroup Failsoft Channel	The system channel designated for a talkgroup when in the failsoft mode
Talkgroup ID	Numerical designation of the talkgroup in decimal and/or hexadecimal
Talkgroup Name	Name of the talkgroup as it is programmed into the system
TDOSHS	Tennessee Department of Safety & Homeland Security
TEMA	Tennessee Emergency Management Agency
THP	Tennessee Highway Patrol
THSP	Technical Specialist
TIA	Telecommunications Industry Association
TRIG	Tennessee Radio Interoperability Guide

Item/Acronym	Definition
Trunking/Trunked	The automatic and dynamic sharing of a number of communications channels between large numbers of radio users
TVRCS	Tennessee Valley Regional Communications System
UHF	Ultra High Frequency – Range of 300 to 3,000 MHz for public safety LMR usually refers to two bands. 380 to 460 MHz (low) and 460 to 512 MHz (high).
UPS	Uninterruptible Power Source – a battery back-up device that provides emergency power to connected equipment when utility power is not available.
VHF	Very High Frequency – For public safety LMR, usually refers to VHF High Band with a range of 136 to 164MHz. VHF Low Band has a frequency range below 100MHz.
VOAD	Volunteer Organization Assisting in Disasters
Zone	An area in the radio / template containing positions for 16 individual talkgroups or conventional radio channels which is normally labeled by an acronym that closely represents the owner agency