EXHIBIT "B" – ATTACHMENT 1A

Regional Public Safety Intranet Demarcation Points

Regional Dispatch Center

RPSI Portion	Demarc	COUNTY Responsibility	CITY Responsibility
Trunked Radio System	Gold Elite Console(s)	Infrastructure and software up to and including the COUNTY-owned Gold Elite/P25 IP based Radio Console(s) located in the Regional Dispatch Center.	All mobile and portable radio subscriber units including any software required to operate on the RPSI Trunked Radio System; and any advanced features and other monitoring equipment, as desired.
CAD System	CITY LAN	Infrastructure and software up to and including the CAD server, Regional dispatch console workstations, Regional Dispatch CAD client licenses, and the needed communications via the RPSI.	All extended CITY LAN equipment along with software, client licenses, peripheral equipment to provide communications to CITY "read only" CAD workstations and all existing interfaces. (Future interfaces to the COUNTY-supplied systems do not apply.)
AVL System	CITY LAN	Infrastructure up to and including the AVL server, regional client desktop software licenses, and the needed communications via the RPSI.	All extended CITY LAN equipment along with software, client licenses, peripheral equipment to provide communications to CITY "read only" CAD workstations and all existing interfaces. (Future interfaces to the COUNTY-supplied systems do not apply.)
Advanced Tactical Mapping	CITY LAN	Infrastructure up to and including the advanced tactical mapping servers, regional standard desktop client software licenses, and the needed communications via the RPSI.	All extended CITY LAN equipment along with software, client licenses, peripheral equipment to provide communications to CITY "read only" CAD workstations and all existing interfaces. (Future interfaces to the COUNTY-supplied systems do not apply.)
Fire Records Management	CITY LAN	Infrastructure up to and including the Fire Records	Desktop hardware and all LANs connected to the FRMS; non-

RPSI Portion	Demarc	COUNTY Responsibility	CITY Responsibility
System		Management servers and standard software site and client licensing for Fire Records.	standard or customized software desired by CITY.
Law Records Management System	CITY LAN	Infrastructure up to and including the Law Records Management servers.	Desktop hardware and all LANs connected to the LRMS; non-standard or customized software desired by CITY and standard software site and client licensing for Law Records.

EXHIBIT "B" – ATTACHMENT 1B

Regional Public Safety Intranet Demarcation Points

Non-Dispatch Facility

RPSI Portion	Demarc	COUNTY Responsibility	CITY Responsibility
CAD System	CITY LAN	Infrastructure up to and including physical network connectivity from the RPSI to a single pre-defined CITY location.	All extended CITY LAN equipment along with software, client licenses, desktop workstations, peripheral equipment to provide communications to CITY "read only" CAD workstations and all existing interfaces. (Future interfaces to the COUNTY-supplied systems do not apply.)
Advanced Tactical Mapping	CITY LAN	Infrastructure up to and including physical network connectivity from the RPSI to a single pre-defined CITY location.	All extended CITY LAN equipment along with software, client licenses, desktop workstations, peripheral equipment to provide communications to CITY ATM workstations and all existing interfaces. (Future interfaces to the COUNTY-supplied systems do not apply.)
Fire Records	CITY LAN	Infrastructure up to and	Desktop hardware and all LANs

RPSI Portion	Demarc	COUNTY Responsibility	CITY Responsibility
Management System		including physical network connectivity from the RPSI to a single pre-defined CITY location. FRMS standard site and client desktop software licenses will be provided from COUNTY to CITY.	connected to the FRMS; non-standard or customized software desired by CITY.
Law Records Management System	CITY LAN	Infrastructure up to and including physical network connectivity from the RPSI to a single pre-defined CITY location.	Desktop hardware and all LANs connected to the LRMS; non-standard or customized software desired by CITY and standard software site and client licensing for Law Records.

EXHIBIT "B" – ATTACHMENT 1C

Regional Public Safety Intranet Demarcation Points

Mobile Data – Law Enforcement

RPSI Portion	Demarc	COUNTY Responsibility	CITY Responsibility
Trunked Radio System	Gold Elite Console(s)	Infrastructure up to the COUNTY-owned Gold Elite/P25 IP Console(s) located in the Regional and/or Non-Regional Dispatch Center.	All mobile and portable radio subscriber units including any software required to operate on the RPSI Trunked Radio System; and any advanced features and other monitoring equipment, as desired.
CAD System	CITY/CITY MDT	Infrastructure up to and including the CAD server and the needed communications via the RPSI.	All extended LAN equipment along with software, client licenses, peripheral equipment to provide communications to CITY CAD MDT's and all existing interfaces. (Future interfaces to the COUNTY-supplied systems do not apply.)
AVL System	COUNTY's Server	Infrastructure up to and including the AVL server;	All vehicle-related equipment and any remote monitoring

RPSI Portion	Demarc	COUNTY Responsibility	CITY Responsibility
		and the needed communications via the RPSI.	equipment and software
Law Record Management System	COUNTY infrastructure	Infrastructure up to and including the Law Records Management servers.	All vehicle Equipment including laptop, modem, cabling, associated mounting hardware, antenna – and any monitoring Equipment and standard software site and client licensing for Law Records. Non-standard or customized software is also the responsibility of the CITY.

EXHIBIT "B" – ATTACHMENT 1D

Regional Public Safety Intranet Demarcation Points

Mobile Data - Fire Rescue Frontline Vehicles

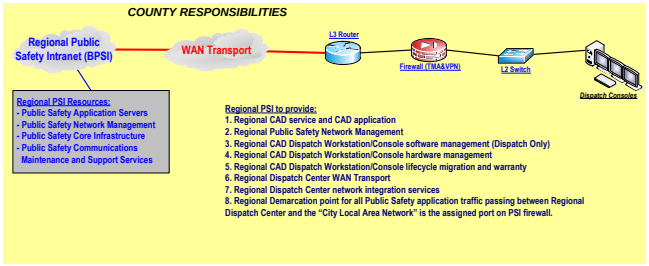
RPSI Portion	Demarc	COUNTY Responsibility	CITY Responsibility
Trunked Radio System	Gold Elite Console(s)	Infrastructure up to the COUNTY-owned Gold Elite/P25 IP Console(s) located in the Regional and/or Non-Regional Dispatch Center.	All mobile and portable radio subscriber units including any software required to operate on the RPSI Trunked Radio System; and any advanced features and other monitoring equipment, as desired.
CAD System	CITY LAN	Infrastructure and software up to and including the CAD server, MDT hardware, MDT regional CAD client software licenses, and the needed communications via the RPSI.	All vehicle related peripheral equipment and any monitoring equipment. Non-Regional or customized software desired by CITY. (Future interfaces to the COUNTY-supplied systems do not apply.)

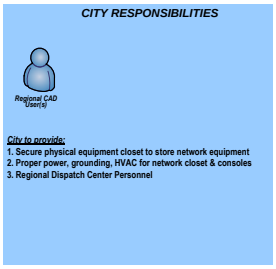
RPSI Portion	Demarc	COUNTY Responsibility	CITY Responsibility
AVL System	Frontline Vehicle	Infrastructure up to and including the AVL server, and GPS devices located in Fire Rescue frontline vehicles.	All vehicle-related peripheral equipment and any remote monitoring equipment and software.
Mobile Data Terminals	Frontline Vehicle	COUNTY will assume capital and lifecycle procurement of MDT's and associated regional standard software for Fire Rescue frontline vehicles.	All vehicle related peripheral equipment and any monitoring Equipment. CITY responsible for wireless modems and recurring operating costs. Non-regional or customized software desired by CITY.
Fire Record Management System	COUNTY infrastructure	COUNTY infrastructure up to and including the FRMS Server and the needed communication interfaces via the RPSI.	Acquisition of FRMS standard site and client mobile software licenses will be the responsibility of CITY. All vehicle related peripheral equipment and any monitoring Equipment. Non-regional or customized software desired by CITY. (Future interfaces to the COUNTY-supplied systems do not apply.)

EXHIBIT "B" – ATTACHMENT 2 (Drawings)

Broward County RPSI: ILA Regional Dispatch CAD DMARC
Broward County - Public Safety Intranet

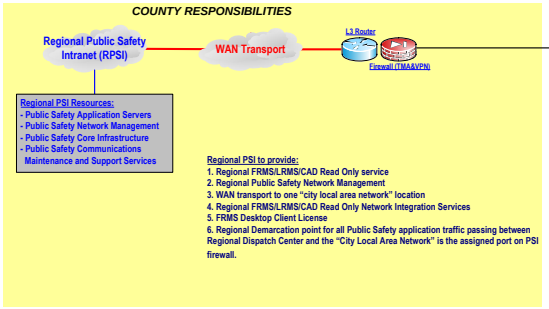
Logical Network Design Overview Regional Dispatch Center
Broward County/City Responsibilities

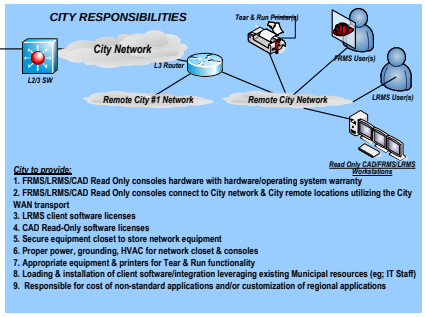




COUNTY – PSI – ILA: Regional Dispatch Center (CAD Demarc's) Sheet 1 of 7

Broward County RPSI: ILA Non-Dispatch Facility Application DMARC
Broward County - Public Safety Intranet
Logical Network Design Overview Non-Dispatch Facility
Broward County/City Responsibilities



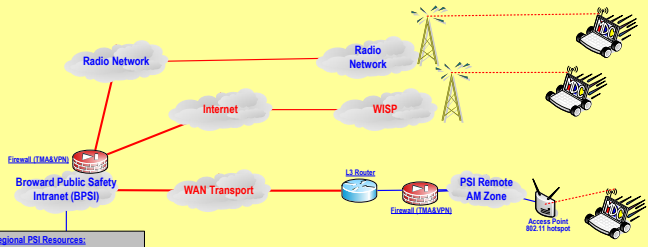


COUNTY – PSI – ILA: Non-Dispatch Facility Application Demarc's Sheet 2 of 7

Broward County RPSI: ILA Mobile Data FR Frontline

Broward County - Public Safety Intranet
Logical Network Design Overview Mobile Data- Fire Rescue
Frontline Vehicles
Broward County/City Responsibilities

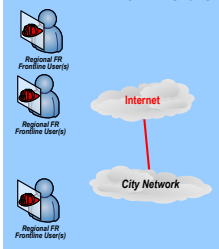
COUNTY RESPONSIBILITIES



Regional PSI Resources:
- Public Safety Application Servers
- Public Safety Network Management
- Public Safety Core Infrastructure
- Public Safety Communications Maintenance and Support Services

Regional PSI to provide:
1. Regional Applications Service (CAD, PMDC, FRMS, AVL, ATM)
2. Regional Public Safety Network Management
3. Regional Public Safety Mobile Data Terminal Software Management (PSI Applications Only)
4. Regional Public Safety Mobile Data Terminal Hardware Management
5. Regional Public Safety Mobile Data Terminal Lifecycle Migration and Warranty
6. WAN Transport to one "CITY Local Area Network" location
7. Regional Public Safety Network Integration Services
8. Vehicular GPS hardware and installation services to facilitate "closest unit response"
9. Standard PSI Application software client licenses (CAD, PMDC, AVL, ATM)
10. Services for loading & installation of regional client software/integration
11. Regional Demarcation point for all Public Safety application traffic passing between Regional Dispatch Center and the "City Local Area Network" is the assigned port on PSI firewall.
12. Regional Demarcation point for all approved application traffic being made available via the Radio Network (modem) is the private RF infrastructure. Radio Infrastructure is the responsibility of COUNTY and the Radio Modem is the responsibility of the CITY.

CITY RESPONSIBILITIES



City to provide:
1. Mobile WAN transport for Modem (public/private)
2. The wireless modem (aircard) hardware and recurring expense is the responsibility of CITY.
3. If CITY is a remote Air/Mobile hotspot then secure equipment closet to store network equipment
4. CITY to provide access to their jurisdictional Local Area Network for connectivity to CITY centric applications
5. FRMS Mobile Client Licenses
6. Proper power, grounding, HVAC for network closet & consoles if needed
7. Non-standard applications and/or customization of regional applications
8. Services for loading & installation of non-regional or non-standard client software/integration
9. Standard vehicles and peripherals to support Mobile Data Terminals (eg; Fire Rescue Front Line Vehicles)

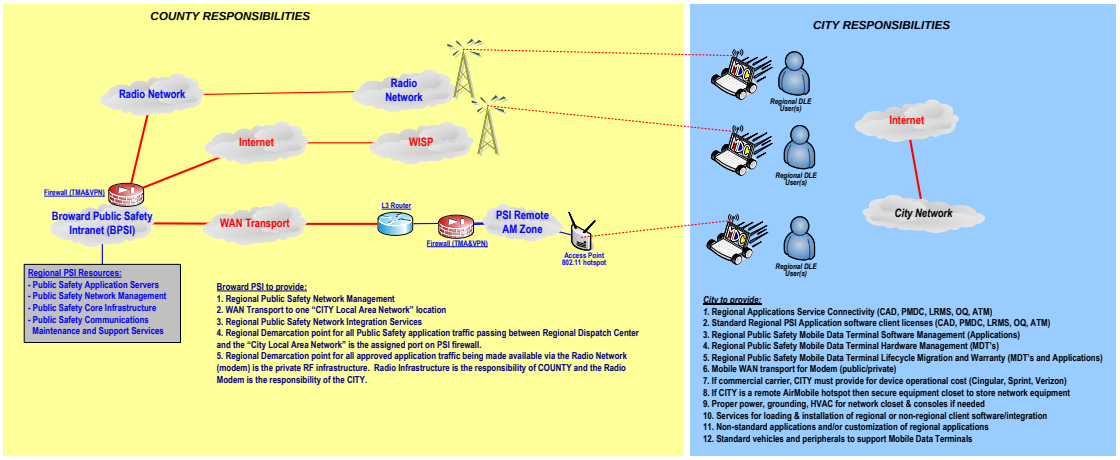
COUNTY – PSI – ILA: Mobile Data – Fire Rescue Frontline Vehicles

Sheet 3 of 7

Broward County RPSI: ILA Mobile Data Law Enforcement

Broward County - Public Safety Intranet

Logical Network Design Overview Mobile Data- Law Enforcement
Broward County/City Responsibilities

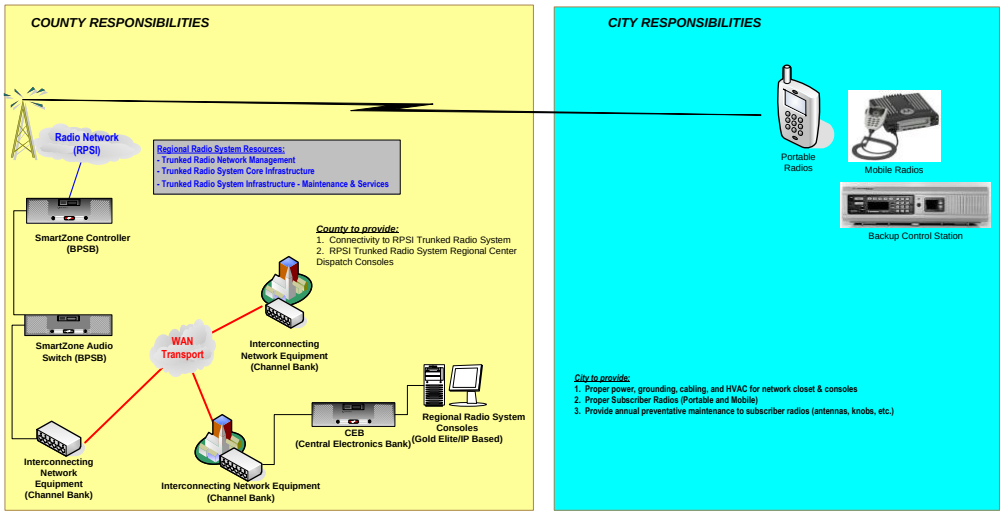


COUNTY – PSI – ILA: Mobile Data – Department of Law Enforcement

Sheet 4 of 7

Broward County-Radio Network: ILA Radio Demarc – Direct Subscribers

RPSI – Trunked Radio System
Logical Network Design Overview Broward County Radio System
Broward County/City Responsibilities

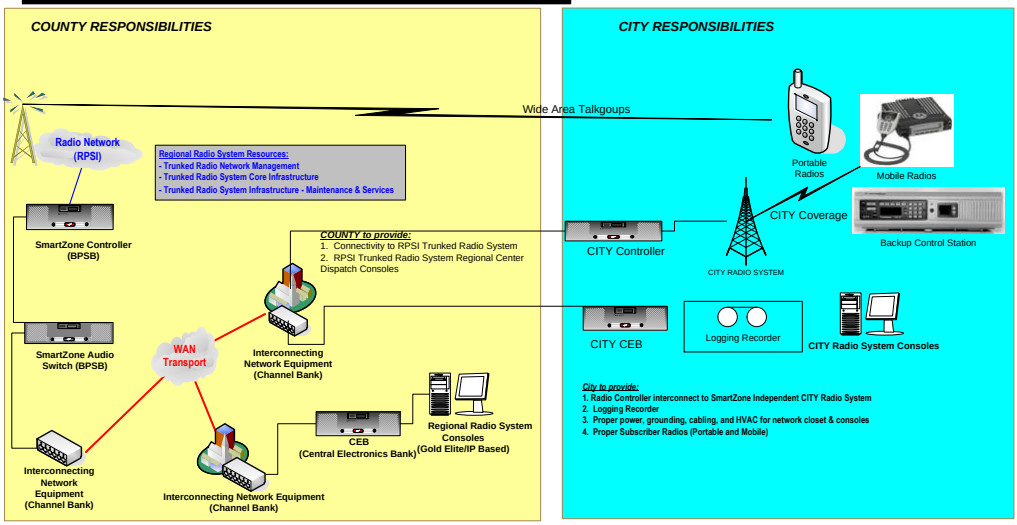


COUNTY – RADIO – ILA: Trunked Radio System – Direct Subscribers

Sheet 5 of 7

Broward County Radio Network: ILA Radio Demarc – Indirect Subscribers

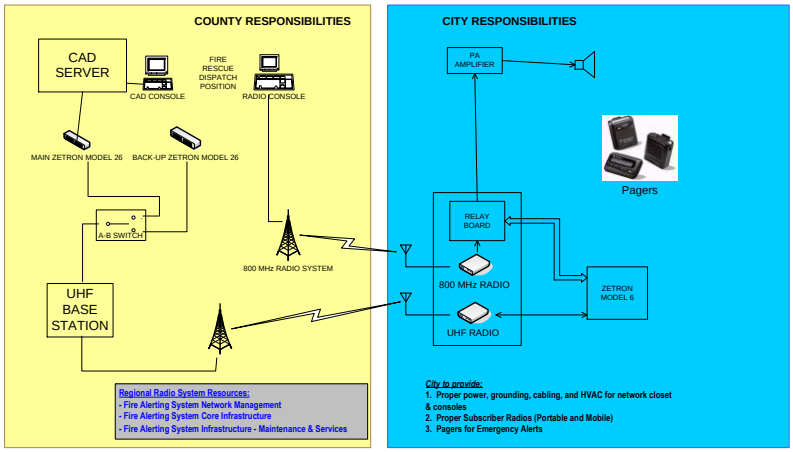
RPSI – Trunked Radio System
Logical Network Design Overview Broward County Radio System
Broward County/City Responsibilities



COUNTY – RADIO – ILA: Trunked Radio System –Indirect Subscribers | Sheet 6 of 7

Broward County-Station Alerting: ILA Fire Station Alerting System Demarcation Drawing

RPSI – Fire Station Alerting System
Logical Network Design Overview Broward County Radio System
Broward County/City Responsibilities



COUNTY – STATION ALERTING – ILA: Regional Fire Station Alerting | Sheet 7 of 7

EXHIBIT D

Change Management Request Procedure

Broward County
Office of Communications Technology

Change Management Request Procedure

Introduction

This document defines the Change Management Request (CMR) process for any component(s) that make up the Regional Public Safety Intranet providing delivery of services to end-users. The CMR process will be used to specify the times and conditions when designated tasks can be performed as maintenance on all software and equipment affiliated with the Regional Public Safety Intranet including but not limited to the Public Safety Network (PSN), Trunked Radio System, Computer Aided Dispatch (CAD) System, LRMS, FRMS, PMDC, UDT/DSS, E-911, etc.

Objective

The objective of the CMR process is to implement maintenance and expansion guidelines that will assure system reliability; minimize the impact on end-users and prevent unintended outage conditions.

Definition

The CMR process will be an ongoing activity involved with the scheduling, communication and coordination of maintenance and construction activities impacting the RPSI. This process includes a Request, Review and Approval process. All change and maintenance activities are performed during predetermined and mutually acceptable Maintenance Windows.

Scope

The CMR process should be followed for any installation, equipment and software maintenance activity or any construction activity which either directly or indirectly impacts the Regional Public Safety Intranet.

CMR Process Requirements

All scheduled change and maintenance activities will require completion of an electronic CMR form and must conform to the following criteria:

- All work requests that impact directly or indirectly the end-users of Public Safety Mission Critical applications must be thoroughly documented in the CMR forms and sent as an e-mail attachment to: octchangemanagement@broward.org.

- COUNTY's Office of Communication Technology (OCT) will review all requests and obtain consensus from Operations and from all impacted end-users on scheduling the Maintenance Window for the request.

- Activities will be scheduled and performed only during predefined or mutually acceptable Maintenance Windows.

- The Requestor submitting the Method of Procedure (MOP) form must identify the scope of the associated outage and a best estimate of the duration of the activities involved in the project. Stop times must take into account the time needed to restore the system to an operational state.

- Following COUNTY OCT approval of the submitted Method of Procedure (MOP), a project coordination meeting involving representatives of all involved or impacted parties will be scheduled by the assigned OCT Program Manager prior to the start of the scheduled work.

MOP Requirements

- The MOP must clearly state the objective(s) of the work to be performed; the parties performing the work; the parties impacted by the work and the steps to be completed by each party.

- A Maintenance Window identifying a clear Start and Stop time and a work flow schedule must be developed and included as part of the MOP.

- The scheduled work must follow the predetermined schedules identified in the MOP, and, as previously noted, stop times must take into account the time needed to restore the system to an operational state.

- The MOP must clearly identify the Program Managers responsible for coordination of the activity and provide telephone numbers and any other relevant contact information.

- The MOP must include an escalation list with notification time frames should unforeseen problems occur that would result in an outage extending beyond the scheduled Maintenance Window.

- The MOP must include a fallback plan should the original plan not work.

Emergency Maintenance

Emergencies by their nature are not a part of the CMR process, but can seriously impact end-users and any scheduled maintenance activities.

In the event of an emergency outage, both the affected end-user and first responder must notify the designated on-call person for the Office of Communications Technology (OCT). An on-call list will be provided to each

911/Dispatch Center Duty Officer and Manager. The OCT contact will be responsible for the following actions:

- Identifying and assigning resources to work the emergency.

- Acting as a liaison between the maintenance provider and the 911/Dispatch Center Duty Officer and Manager for the duration of the outage or service degradation.

- Documenting response times and actions taken, followed by generating an after-action report.

The maintenance provider(s) responding to an outage or service affecting emergency must take the following measures following notification:

- Upon notification, use remote access to diagnose and repair the problem or arrive on site within the contracted time frames of the responder's maintenance agreement.

- Assess the nature and scope of the problem.

- Notify the COUNTY OCT on-call person of all actions to be taken and provide the best possible estimate of the duration of the outage or service degradation.

- Notify the COUNTY OCT on-call person of any break in maintenance activity prior to completion of the repair for any reason.

- Provide periodic updates for extended outages.

- Document each step of the repair/troubleshooting process as it is performed.

- Within 24 hours of completion of a repair, provide a written summary of the problem and the measures taken to repair the problem and (if relevant) prevent similar future outages.

- COUNTY OCT managers will review the submitted documentation and on a case by case basis schedule a debriefing session to review the steps taken to resolve the problem and suggest changes or improvements for responding to future unscheduled outages.

Maintenance Windows

- The standard weekday Maintenance Window for Public Safety Communications Operations is 12:01 AM – 06:00 AM Sunday through Thursday or as otherwise specified by the Operations managers.

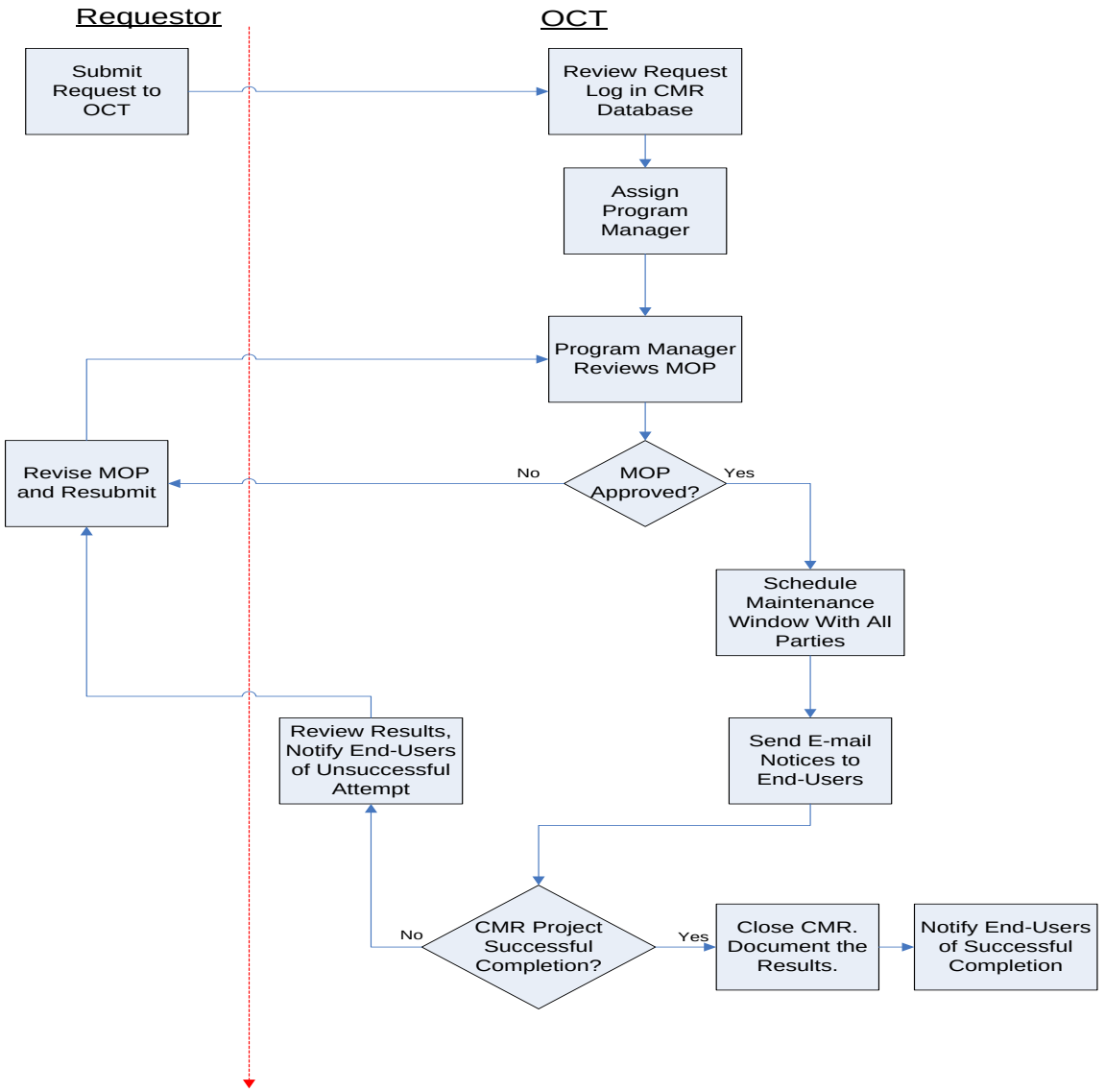
- The standard weekend Maintenance Window for Public Safety Communications Operations is 5:01 AM – 02:00 PM Saturday and Sunday or as otherwise specified by the Operations managers.

- A CMR must include sufficient time to perform a back-out of the change within the Window timeframe and restore systems to their normal operational state.

- A CMR that requires work to be performed outside the standard Maintenance Windows must include justification for performing the work during a non-standard window and be approved by COUNTY's OCT.

Change Management Request

Process Work Flow



Type	Risk Impact Level	Definition	Lead Time	MOP Required	Actions Description
FYI	**Non-Service Affecting**	**Prep work activity which has low risk to end-users of Public Safety Mission Critical applications.**	**Minimum 2 days**	**No**	**FYI as needed.**
Scheduled	**Potential-Service Affecting**	**Any activity that may impact end-user access to Public Safety Mission Critical applications.**	**Minimum 5 days**	**Yes**	**Notify all End-Users and Support Management**
Scheduled	**Service Affecting**	**Includes any activity which will result in the loss or degradation of accessibility to end-users of one or more Public Safety Mission Critical applications.**	**Minimum 10 days**	**Yes**	**Obtain written or e-mail approval from Management.** Provide Written Notification to all affected End-Users. Obtain Written Approval of all affected End-Users.
Scheduled	**Outage Required**	**Any work which will necessitate a total outage of one or more of the Public Safety Mission Critical applications or the Public Safety Wide Area Network, or any extremely high risk activity which may inadvertently cause an outage.**	**Minimum 10 days**	**Yes**	**Obtain written or e-mail approval from Management.** Provide Written Notification to all affected End-Users. **Obtain Written Approval of all affected End-Users.**
Emergency	**Service Affecting or Outage Required**	**The unscheduled outage of one or more Public Safety Mission Critical applications or the Public Safety Wide Area Network.**	**None**	**No**	**Requires immediate management and End-User notification and a debriefing meeting once the problem has been resolved.**

End-User Notification

Not less than ten (10) business days prior to an approved CMR project affecting the Regional Public Safety Intranet, the COUNTY OCT project manager must notify all end-user management by e-mail of the pending activity with all CMR and MOP documentation attached. The e-mail should summarize the attached documentation but must include:

- A list of all affected end-users.
- A generic statement of nature of upgrade or maintenance procedure and the operational need to make the change.
- The Maintenance Window, date and time the work will be performed including the projected end time.
- A generic impact statement that identifies the nature of the work being performed; the impact of the work on the end-user while the work is performed and the effect of the work on the restored system or application.
- Telephone numbers of project managers and key staff involved in the activity.

Approval Authority

Any and all activities being performed must be supported by an approved CMR document.

Broward County

Office of Communications Technology (OCT)

Change Request Form

Note: Complete and submit to the Broward County Office of Communications Technology at OCTChangeManagement@broward.org. All Change Requests submitted prior to Wednesday are reviewed during the Thursday morning conference calls and either approved or returned for modifications. Please allow a minimum of ten (10) business days from the date of approval for your Maintenance Window to be scheduled. Any work performed on the Public Safety Communications Network, its supporting infrastructure, or the application servers must be documented and approved in a CMR.

Today's Date and Time:	
Requestor Name:	
Requestor Company Name or Agency:	
Requestor E-Mail:	
Requestor Phone Number:	Office:
	Mobile:
Briefly describe the Work to Be Performed:	
Identify End-Users & sites impacted by the work to be performed:	

What is the expected and desired end result of the Work to be Performed?	
Identify any loss or degradation of functionality and the impact on end-users during the Maintenance Window:	
Identify your On-Site Contact during the scheduled Maintenance Window:	Name & Contact Number:
Requested Maintenance Window for Work to be Performed:	Start Date & Time: Stop Date & Time:
Approved Maintenance Window for Work to be Performed:	Start Date & Time: Stop Date & Time:
Maintenance Window Approved By:	Date:
Assigned MOP Tracking Number:	

Method of Procedure – for Primary Contractor or Service Provider Note: An MOP must be completed for each Contractor or Service Provider working on a specific project. Use electronic attachments as needed.	
Company or Agency Name:	
Project Manager Name:	
Project Manager Office Phone Number:	
Project Manager Mobile Phone Number:	
Project Manager E-Mail:	
Detailed Project Description	
Specify each step in the MOP Work Process. Attach additional pages or any supporting documents as needed:	
Describe back-out and restoration plans if stated project goals are not achieved within the allotted Maintenance Window:	

OCT to complete Items 1 through 10 Below:		
(1) OCT Contact for Project:	(2) Name:	
	(3) Mobile Phone Number:	
	(4) E-Mail:	
(5) MOP Type:	(6) FYI – Non-Service Affecting: ☐	
	(7) Scheduled – Potential Service Affecting: ☐	
	(8) Scheduled – Service Affecting: ☐	
	(9) Scheduled – Outage Required: ☐	
	(10) Emergency: ☐	
Reviewer Comments:		
Method of Procedure Approved By:	Date Approved	

EXHIBIT "E"
Project Charter

PROJECT CHARTER

*[**Note**: All fields in **blue text** must be filled in.]*

1. General Project Information			
Project Name:			
Department/Agency Sponsor:			
• ***What department is the primary proponent of this project? (*Enter one.*)***			
• Who, within that department, is the Project Sponsor? (*Note: This person must be a decision-maker with the authority to commit department resources.*)			
• Is this a Regional Project, i.e. does it have significant impact on regional applications or resources (Y/N)?			
Department Co-Sponsor:			
Department/Agency Project Rank:			
If this project is mandated or is required for continued business operation:	**Mandated by whom?**		
	Impact of not meeting mandate?		

Document History			
Version	Date	Author	Reason for Change

2. Stakeholders

	Name	*Department*	*Telephone*	*E-mail*
Agency Lead:				
Regional Applications / PSI Manager:				
Project Lead:				
Others: **Key Players from the City**				
Agency Lead:				
TechLead:				
Tech Lead:				

3. Vendor Contacts

Name	*Company / Role*	*Telephone*	*E-mail*

4. Project / Service Description

Project Purpose / Business Justification
Objectives (in business terms)

4. Project / Service Description

Deliverables

Clear Statement of What This Project Will Not Include

Project Success

Project Milestones

Major Known Risks (including significant Assumptions)

Risk Rating (Hi, Med, Lo):

Constraints

External Dependencies

4. Project / Service Description

Project Strategy

List of events that should take place in chronological order:

5. Financial / Resources Information

Funding Source **Operating Budget, Capital Budget, Grant, Other.**

Estimate of Implementation Cost

Return-on-Investment (ROI) Data

Estimate time required of Multi-Department Staff

Role	Hours needed

Estimate time required of other Organization Staff

Role	Hours needed

6. Estimated Total Cost of Ownership (TCO) 5-Year – Provider (BC-OCT)

The OPEX figures below only represent the provider capex and opex based on hardware, software, and professional services.

Calendar Year (1, 2, 3) or Fiscal Year (2012-13, 2013-14)	Capital ($U.S.)	Operational ($U.S.)
2012-13	0	0
2013-14	0	0
2014-15	0	0
2015-16	0	0
2016-2017	0	0
Totals	***$0***	***$0***

7. Estimated Total Cost of Ownership (TCO) 5-Year – Client (City)

The OPEX figures below only represent the monthly recurring cost for aircards and does not represent the annual O&M expense for software and hardware devices.*

Calendar Year (1, 2, 3) or Fiscal Year (2009-10, 2010-11)	Capital ($U.S.)	Operational ($U.S.)
2012-13	$0.00	$0.00
2013-14	$0.00	$0.00
2014-15	$0.00	$0.00
2015-16	$0.00	$0.00
2016-17	$0.00	$0.00
Totals	***$0.00***	***$0.00***

8. Sourcing Strategy

Organization-Managed and Hosted		
Vendor-Managed and Hosted		
Organization-Managed, Vendor-Hosted		
Vendor-Managed, Organization-Hosted		

9. Acquisition Strategy

Sole-Source / Amend Contract		
RFP / Competitive Bid		
In-House / Custom-Develop		
Other:		

10. Types of Vendor Assistance

Turnkey Solution			Supplemental Staffing (Time/Materials)		
Vendor-Assisted (Fixed Price)			Hardware / Software		
Other:			None / Not Applicable		

11. Sign-off

	Name	Title	Signature	Date (MM/DD/YYYY)
Business Sponsor				
Business Sponsor				
Program Manager				
Agency Sponsor				
Agency Sponsor				

12. List of Addenda

Document Name	Filename and Location

13. Notes / Comments

EXHIBIT "F" – ATTACHMENT 1
Service Level Agreements
Terms and Conditions

INTRODUCTION

This purpose of this Service Level Agreement (SLA) is to clarify the mutual expectations of the CITY and the COUNTY. Changes in software and hardware architecture make it imperative that all members understand their mutual responsibilities.

1.0 MAINTENANCE SERVICE AND SUPPORT

1.1 Maintenance Service and Support being provided are based on the Severity Levels as defined below. Each Severity Level defines the actions that will be taken by COUNTY for Response Time (MTTR), Resolution Time, and Resolution Procedure for reported errors. Response Times for Severity Levels 1 and 2 are based upon voice contact by CITY, as opposed to written contact by e-mail, facsimile or letter. Should delays by CITY prevent scheduling of downtime to resolve an issue, COUNTY will not be held responsible for Resolution time frames listed below.

SEVERITY LEVEL	DEFINITION	MTTR (Mean Time To Respond)	TARGET RESOLUTION
1	Failure/Outage occurs when the system is not functioning which prohibits continuance of mission critical operations.	≤30 minutes of initial voice notification*	Resolve within 24 hours of initial notification*
2	Failure occurs when an element in the system is not functioning that does not prohibit continuance of normal daily operations.	≤ 24 business hours of initial voice notification.*	Resolve within 5 standard business days of initial notification*
3	An Inconvenience occurs when software or hardware causes a minor disruption in the way tasks are performed but does not stop workflow.	≤48 business hours of initial notification	Resolution determined on a case by case basis.

*Does not apply to "READ-ONLY" CAD Systems

1.2 The CITY System Administrator shall conduct a preliminary error review to verify a problem, determine if such is the direct result of a defect in Hardware, Software, or other and the direct conditions under which the problem occurred, identify the applicable urgency rating scale by which errors, problems, and other issues are scheduled ("Severity Level"), and ascertain that errors are not due to an external system, data link between systems, or network administration issue prior to contacting COUNTY.

1.3 CITY shall assign an initial Severity Level for each error reported, either verbally or in writing, based upon the Severity Levels defined above. Severity Level 1 or 2 problems should be reported verbally to the COUNTY by CITY Representative or System Administrator.

COUNTY will notify the CITY if COUNTY makes any changes in Severity Level (upgrade or downgrade) of any CITY-reported problem.

1.4 COUNTY shall provide telephone support for maintenance issues 24 hours per day, 7 days a week (24 x 7).

1.5 All requests for support for the products specified in this Exhibit will be logged with the COUNTY Customer Support Center ("CSC") via telephone at 1-954-357-8686 or email at selfhelp@broward.org

1.6 COUNTY will provide CITY with a resolution within the appropriate Resolution Time and in accordance with the assigned error Severity Level when COUNTY diagnostics indicate that the error is present. Additionally, COUNTY will verify: (a) the Hardware and Software operates in conformity to the System Specifications, (b) the Hardware and Software is being used in a manner for which it was intended or designed, and (c) that the Hardware and Software is being used only with COUNTY approved Hardware or Software. Resolution Time period shall not begin to run until such time as the verification procedures occur. COUNTY will continue to provide service support under this Inner Local Agreement until final resolution is determined.

1.7 Should COUNTY determine that it is unable to correct such reported error within the specified Resolution Time, COUNTY will upgrade and escalate its procedure and assign such personnel or designee to correct such error. This will include automatic problem call escalation to appropriate levels of COUNTY Management.

1.8 Any and all Maintenance Service provided for herein shall be warranted under the following terms and conditions:

a) Third party hardware, software, and any other related supplies shall conform to any and all applicable industry approved technical, functional, and performance specifications;

b) The System is free of modifications and alterations which have not been pre-approved by COUNTY.

c) The System is free of any evidence of negligence, misuse and/or abuse, intentional or otherwise.

1.9 Unless otherwise specified herein, any and all suspected errors will be investigated and corrected at COUNTY Facilities. COUNTY shall decide whether on-site correction of any Hardware and Software error is required.

1.10 Any third party equipment supplied by COUNTY shall be guaranteed by the manufacturer's warranty for that equipment.

2.0 RECORD –KEEPING AND REPORTING RESPONSIBILITIES

2.1 COUNTY will provide verbal and written status reports on Severity Level 1 troubles. Written status reports on outstanding errors will be provided to CITY System Administrator on a monthly basis upon request.

2.2 COUNTY shall provide annual account reviews to include: a) service history of site; b) downtime analysis; and c) service trend analysis.

2.3 COUNTY will prepare the following reports (for PremierCAD software only), to include:

a) System Analysis	MEASURE:	Evaluate disk and CPU load
	PEEK:	Evaluate memory availability and use
	VIEWSYS:	Evaluate use and availability of PCBs
	EMSA/TMDS:	Review logs for hardware reports
	File Sizing:	Review file sizing on changeable files

b) Pathway Analysis — Evaluate effectiveness of system configuration for current load.
Evaluate TCP/Server statistics.
Evaluate efficiency of server class maximum and minimum settings.

c) Performance Analysis — TMX Timings: Evaluate application response times

d) Printrak Technical Support Analyst. Based on the Annual System Performance Review and Reports, the Printrak Technical Support Analyst will review findings and recommend software or hardware changes to improve overall operations.

3.0 MISCELLANEOUS

3.1 When COUNTY performs service at the System location, CITY agrees to provide COUNTY, at no charge, a non-hazardous environment for work with shelter, heat, light, and power and with full and free access to the System.

3.2 CITY will provide all information pertaining to the CITY owned hardware and software elements of any equipment with which the System is interfacing that enable COUNTY to perform its obligations under this Service Agreement.

3.3 It is not required that parts furnished by COUNTY be newly manufactured. COUNTY warrants such parts to be equivalent to new in performance. Parts replaced in the course of repair shall, at the close of maintenance, become COUNTY's property.

3.3 CITY will provide a qualified System Administrator for the Printrak System Portion to perform all functions as defined in Printrak's Systems Administrator's guide which has been provided to the CITY under separate cover.

3.4 Upon the expiration or earlier termination of this Agreement, CITY and COUNTY shall immediately deliver to the other Party, as the disclosing Party, all Confidential Information of the other, including any and all copies thereof, which the other Party previously provided to it in furtherance of this Agreement. Confidential Information shall include: (a) Proprietary materials and information regarding technical plans; (b) any and all other information, whether in a softcopy or hardcopy medium, including but not limited to data, developments, trade secrets and improvements that is disclosed in any form by COUNTY to CITY; (c) all GIS, address, telephone, or like records and data provided by CITY to COUNTY that is required by law to be held confidential.

3.5 This Service Level Agreement does not grant directly, by implication, or otherwise, any ownership right or license under any patent, copyright, trade secret, or other intellectual property including any intellectual property created as a result of or related to the products sold or Services performed under this Service Level Agreement.

4.0 SOFTWARE UPDATES

COUNTY shall provide software updates as defined below:

4.1 Supplemental Release is defined as a minor release that contains primarily error corrections to an existing Standard Release. It may also contain limited improvements that do not affect the overall structure of the Software. Supplemental Releases can be installed remotely. Supplemental Releases are identified by the third digit of the three-digit release number, shown here as underlined: "1.2.3".

4.2 Standard Release is defined as a major release of Software that contains product enhancements and improvements such as new databases, modifications to databases, new server/requesters, etc., and may involve file and database conversions, System configuration changes, hardware changes, additional training, modifications of Software license terms, on-site installation, and System downtime. Standard Releases are identified by the second digit of the three-digit release number, shown here as underlined: "1.2.3".

4.3 Product Release is defined as a major release of Software considered to be the next generation of an existing product or a new product offering. Product Releases are identified by the first digit of the three-digit release number, shown here as underlined: "1.2.3".

4.4 The CITY will not be required to pay any additional fees for COUNTY provided Software Releases.

4.5 At CITY's request, COUNTY will provide a current list of compatible hardware operating system releases. A list of Software Supplemental or Standard Releases will also be made available at no charge to CITY.

4.6 CITY must maintain all hardware and software connected to the COUNTY's network to the latest compatible revisions.

5.0 ADDITIONS AND CHANGES

5.1 The CITY may request an enhancement to System functionality. Enhancement requests are submitted to COUNTY Office of Communications Technology (OCT) for review. If OCT accepts the enhancement request, request will be referred to the Program Management Team for possible inclusion in a future project. COUNTY OCT will provide a response to the enhancement request within ninety (90) standard business days upon written receipt of initial request. If accepted, a proposed Project Plan will be furnished with any applicable enhancement fee. The CITY may choose to pay for an enhancement request that has been accepted by Program Management but is not viewed as a high enough priority to include in a release.

6.0 ACCESS

6.1 The CITY agrees to maintain any and all electrical and physical environments in accordance with System manufacturer's specifications.

6.2 The CITY agrees to ensure System accessibility, which includes physical access to building as well as remote access. Remote access is required and will not be substituted with on-site visits if access is not allowed or available.

7.0 EXCLUSIONS

7.1 Maintenance Service and Support not listed in this SLA are excluded, and COUNTY shall not be liable under this Agreement for such services. Exclusions consist of, but are not limited to:

a) Any service work required due to incorrect or faulty operational conditions, including but not limited to equipment not connected directly to an electric surge protector, equipment used in a non-office environment, and equipment not properly maintained in accordance with guidelines set forth in the manufacturer's User's Guide;

b) The repair or replacement of parts resulting from failure of the CITY's facilities or CITY's personal property and/or devices connected to the System (or interconnected to devices) whether or not installed by COUNTY's representatives;

c) The repair or replacement of Equipment that has become defective or damaged due to physical or chemical misuse or abuse from causes such as lightning, power surges, or liquids;

d) The repair or replacement of any transmission medium, such as telephone lines, computer networks, or the worldwide web, or for Equipment malfunction caused by such transmission medium;

e) Accessories; custom or Special Products; office furniture which includes chair(s) and workstation(s); modified units; or modified software;

f) The repair or replacement of parts resulting from the tampering by persons unauthorized by COUNTY or the failure of the System due to extraordinary uses;

g) Operation and/or functionality of CITY's personal property, equipment, and/or peripherals and any non-COUNTY provided application software including service of any accessory, attachment, or component owned by CITY, whether or not installed by COUNTY;

h) Removal, relocation, and/or reinstallation of System or any component thereof;

i) Services to diagnose technical issues caused by the installation of unauthorized components or misuse of the System.

j) Operational supplies including, but not limited to, printer paper, printer ribbons, toner, photographic paper, magnetic tapes, any supplies in addition to that delivered with the System, and battery replacement for uninterruptible power supply (UPS).

k) Unauthorized installation of any Software or Hardware modifying Printrak Software and/or the System.

7.2 CITY shall be responsible for payment of any desired service and support not included within the scope of this SLA and such service or support shall be performed at the rates set forth below.

Billable rates are subject to a two (2) hour minimum:

$100 per hour	8 a.m. – 5 p.m. (local time) Monday – Friday
$150 per hour	After 5 p.m. Monday – Friday, and all day on Saturday, Sunday and COUNTY established holidays
Travel Expense	In addition to the above hourly labor rates, all other actual travel related expenses may be charged to CITY.

LIST OF HARDWARE and SOFTWARE

The following lists the System hardware and software items under the ILA coverage/control of COUNTY's area of responsibility:

EXHIBIT "F" – ATTACHMENT 2
Service Level Agreements
Trouble Ticket Workflow

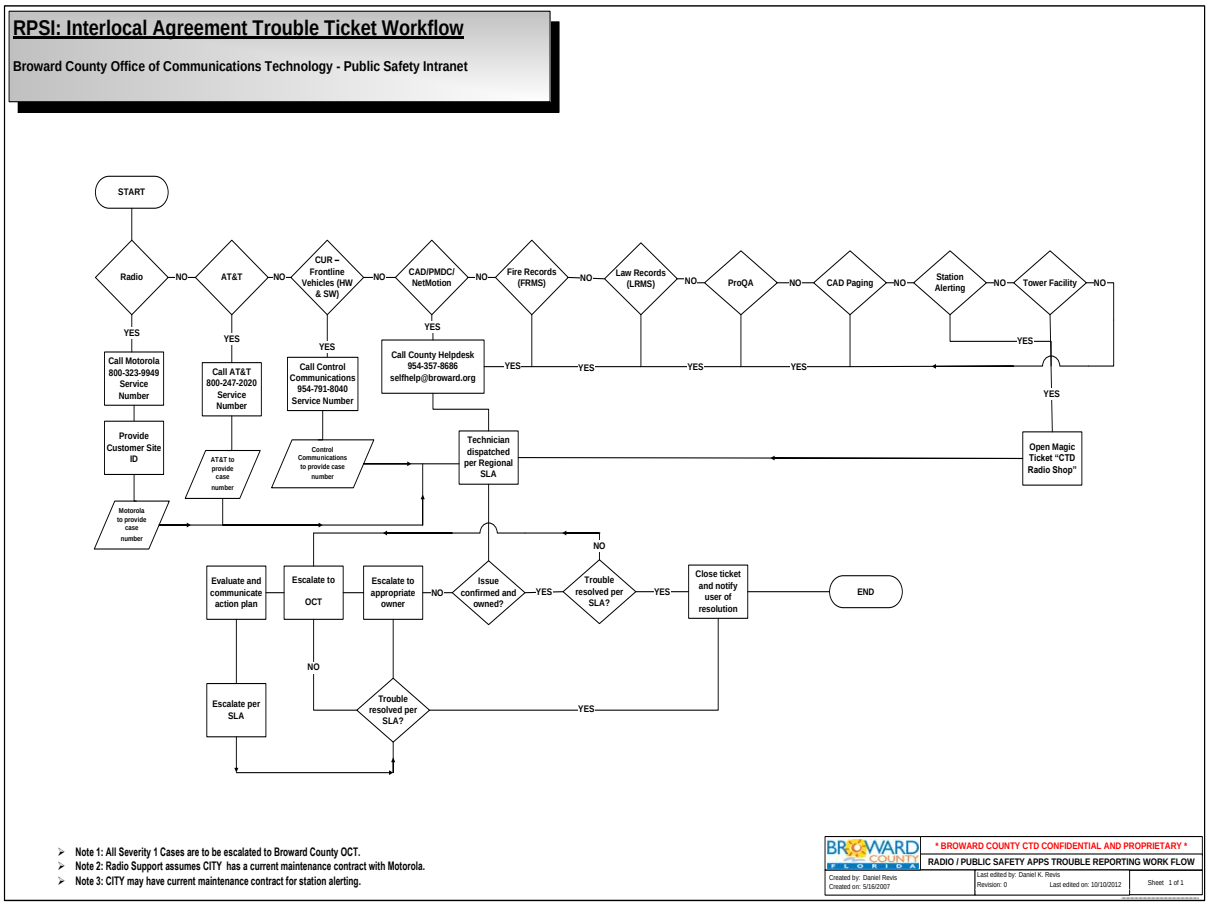


EXHIBIT "G"

Trunked Radio System
Standard Operating Procedures

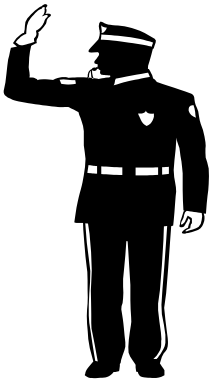
Regional Public Safety

Communications –

Radio Sub-Committee

Standard Operating Procedures

For the Broward County Public Safety Intranet



RPSCC RADIO SUB-COMMITTEE

STANDARD OPERATING PROCEDURES

FOR THE BROWARD COUNTY

PUBLIC SAFETY INTRANET

TABLE OF CONTENTS

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.1 Sub-Section: Procedure Title: **Fleetmap Standards** Date Established: 12/15/06 Replaces Documents Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

The 800 MHz system will contain a large number of talk groups & multigroups to support the various agencies that will be subscribing to the system.

The System has multiple administrating agencies that will be responsible for maintaining the Fleetmaps and system programming for the agencies for which they are responsible.

Talk groups must be configured identically by name in the SmartZone Manager Terminal database, Radio Consoles and the Subscriber Radio. The minimum characters are six (6) and maximum is 14. The Talk Group number of characters will need to be based upon the individual agency's subscriber radio model types used within their fleet.

For the effective management of the system a defined process needs to be used to document the Fleetmap information that each agency is supporting. This information needs to be in a format that is shared with the other administrators.

2. Technical Background:

- **Capabilities:**

The Fleetmap is parameter information programmed into the system infrastructure and into the subscriber radios to control how the radios will behave on the 800 MHz system.

The Fleetmap itself contains the following information:

Fleetmap Information	Definition
Talkgroup	Name of the talkgroup & multigroup as it is programmed into the system
Talkgroup ID	Numerical ID of the talkgroup & multigroup
Owner	The actual “owning” agency of the talkgroup
Description	General description of the talkgroup & multigroup
Multigroup	If the talkgroup is part of a multigroup, this will identify the multigroup
Priority	Priority level of the talkgroup
Admin Agency	The agency that is responsible for the system administration for this talkgroup
Site # access	Will be a listing of the RF sites individually, and if the talkgroup is authorized
Media Access	If media access is permitted for this talkgroup
Global Sharing	The predefined global sharing authorizations

User Groups = The subscriber groups using the talk groups, this becomes a matrix for programming.

The Fleetmap spreadsheet will become a documented matrix of the talk groups in the system and the subscriber groups that are using / sharing these talk groups.

3. <u>Operational Context</u>:

The System Managers will be responsible for managing the Fleetmap information of the users they are representing. This information is also shared with the other system managers; the ID information also must be kept.

4. <u>Recommended Protocol/Standard</u>:

The detailed matrix will be maintained on the system database. An example of the matrix layout is shown in this manual. ***Need to develop the matrix layout.***

Each System Manager will maintain a master Fleetmap spreadsheet containing data on the subscribers for whom they are responsible.

5. <u>Recommended Procedures</u>:

As individual System Managers make updates and changes to their spreadsheets, the spreadsheet will be e-mailed to the Broward County COUNTY’s Office of Communications Technology Radio Communications Manager, the Administrator (for future reference this person will be

referred to as the “Primary Administrator”) of the system. This will allow the Primary Administrator to update the master spreadsheet information easily and provide the information to the other System Managers for reference and integrity of the Fleetmap planning process.

Talk groups that are shared between subscribers of different administrating agencies will be reflected on all the spreadsheets having subscribers using these talk groups. The portion of the System Manager’s spreadsheet containing data on talk group ownership will be considered the master reference for the Talk group.

The disclosure of the Fleetmap configuration information including Talk Group IDs, user IDs, user privileges and other related system information would substantially jeopardize the security of the system from tampering, sabotage, unauthorized use, jamming, hacking, unauthorized access to the contents of confidential voice and data communications, etc. Therefore, the master Fleetmap spreadsheets shall be classified as “Security Information” and “Non-Public Data.” The System Managers may choose to disclose some or all of their own information to their users; however, they shall not disclose other Agencies’ information without prior approval from the responsible System Manager.

6. <u>Management</u>:

The System Managers Group will manage the Fleetmap information and the details of the process for communicating the information.

Standard Operating Procedures (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.2 Sub-Section: Procedure Title: **Talk Group & Radio User Priority** Date Established: 12/15/06 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

The purpose of establishing varying priority levels for talk groups is to assure the most critical talk groups on the system are granted a channel as quickly as possible when the system is experiencing busy conditions.

2. Technical Background:

- **Capabilities**

  The system priorities can be managed at the user level and at the Talk Group level.

- **Constraints**

  All User Priorities will be set at 10, as radio users change talk groups, their effective priority will be set by the Talk Group that they are on.

3. Operational Context:

Priority levels in the system will be managed at the Talk Group level. The goal is to distribute priorities across the systems talk groups in a way that maximizes the ability for critical groups to communicate and minimizes the number of talk groups with high priority. All User Priorities will be set to the lowest priority level, 10.

4. Recommended Protocol/Standard:

The Talk Group owner, or the applicable subsystem owner, shall assign Talk Group priority levels not exceeding the level defined by the criteria below. Talk Group priorities that are assigned to level five or above are subject to the review and audit of the RPSCC Radio Sub-Committee.

Priority 1 Definition – EMERGENCY: Only Emergency Alert calls, i.e. emergency button pressed, will be given the Priority 1 status. Definition of an EMERGENCY means when a public safety radio subscriber encounters a life-threatening situation and needs help by activating their emergency button which then activates their designated dispatcher's radio console with an emergency alert.

Priority 2 Definition – Unassigned

Priority 3 Definition – Unassigned.

Priority 4 Definition – Public Safety Talk Groups

Priority 5 Definition – Low Priority Public Safety Talk Groups

Priority 6 Definition – Unassigned

Priority 7 Definition – Local Government Essential

Priority 8 Definition – Unassigned:

Priority 9 Definition – Local Government Non-Essential

Priority 10 Definition – PRIVATE & INTERCONNECT CALLS: Will be used for Telephone Interconnect Calls, Private Calls as defined by direct point-to-point or radio-to-radio communications that are not carried out within a talk group. This priority will also be used for talk groups that are established for system testing.

5. Recommended Procedures:

N/A

6. Management:

The RPSCC Radio Sub-Committee is responsible for supervision and management of this procedure.

STANDARD OPERATING PROCEDURE (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.3 Sub-Section: Procedure Title: **Telephone Interconnect** Date Established: 12/15/06 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

To manage the use of interconnect on the system. Although this is a useful feature and needed by some users, it must be managed to an appropriate level to protect the primary radio communications purpose of the system.

2. Technical Background:

- **Capabilities**

  Interconnect calls can be placed to individual users of the system, if they are configured for interconnect functionality. Interconnect calls can be placed to talk groups of the system, if the Talk Group is configured for interconnect functionality.

  Interconnect is intended to be a BACKUP functionality to cellular communications and used primarily on an emergency basis.

- **Constraints**

  - An interconnect call will consume an RF channel for the duration of the call.
  - Interconnect calls are half duplex; only one end can talk at a time.
  - A type 1 portable cannot initiate an interconnect call.
  - A type 2 portable can only place calls to numbers that are pre-programmed into the radio.
  - A type 3 portable can place an interconnect call by dialing the number directly.
  - The general public can easily monitor the interconnect calls and they are NOT private or protected in any way.
  - Interconnect shall NOT be utilized to conduct confidential business such as discussing case strategy with the State Attorney's Office.

3. Operational Context:

If a radio user has a need for interconnect, it shall be granted, but the resources impact needs to be carefully managed. Due to the risk of cutting off emergency / life safety communications, the duration of interconnect calls shall be set to a time limit of two (2) minutes. Only one channel within a radio system will be allowed the feature of Telephone Interconnect. The need to make a Telephone Interconnect call must be restricted to emergency and business related use. The CITY of Fort Lauderdale has two (2) channels available for the users that are allowed the Telephone Interconnect feature; however, they do not permit other agencies to utilize their Interconnect resources.

4. Recommended Protocol/Standard:

Interconnect 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, but there may be some users that may require a backup ability to cellular communications.

The priority level for interconnect calls is “10,” this is defined under the priorities standards documents.

The interconnect equipment of the system will be configured to use the “overdial” method of operation, where the incoming calls come into a generic phone number, and then the interconnect ID of the radio is entered to complete the call. The Fort Lauderdale radio system does not support inbound interconnection.

5. Recommended Procedures:

The System Managers need to define and manage the interconnect properties of the RF subsystem(s) that they are responsible for. Each RF subsystem can be configured individually for the number of calls that they will be allowed to simultaneously carry.

6. Management:

The System Managers shall be responsible for following this procedure and monitoring the effect and usage of this resource. If negative impact or excessive usage is determined, interconnect permission will be reconsidered and possibly revoked. Definition of “negative impact or excessive usage is defined as individuals who are reported for using this feature for non-emergency and/or non-business related matters.

STANDARD OPERATING PROCEDURE (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.4 Sub-Section: Procedure Title: **Private Call** Date Established: 12/15/06 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

To manage the use of private call on the system, although this is a useful feature and needed by some users, it must be managed to an appropriate level to protect the primary radio communications purpose of the system.

2. Technical Background:

- **Capabilities**

  Private calls can be placed to individual users of the system, this communication is outside of the Talk Group communications, and is a private communication between two radio users. Console operators can place private calls to the radio users.

- **Constraints**

  - A private call will consume a RF channel for the duration of the conversation.
  - Private calls are half-duplex, only one end can talk at a time.
  - A type 1 portable cannot initiate a private call.
  - A type 2 portable can only place private calls to numbers that are pre-programmed into the radio.
  - A type 3 portable can place a private call by dialing the number directly.
  - Private calls are not recorded.
  - For the duration that a radio user is involved in a private call, the user will not be involved in dispatch / Talk Group communications.
  - The system is not able to restrict the usage of private call on the system, unlike interconnect calls, which can be managed.

3. Operational Context:

The private call resource should primarily be used as a supervisory function, if there is a business need for a radio user to have this ability, it should be granted, but the resource overall needs to be managed to protect the RF resources of the system. This is also a function that dispatch consoles overall would be capable of. Due to the risk of cutting off emergency / life safety communications, the duration of Private Calls must be set to a time limit of two (2) minutes. The number of channels that allow the feature of Private Call will be determined by the individual System Manager. The need to make a Private Call must be restricted to emergency and business related use. Radio users of the Private Call feature must understand that when this feature is being used, they cannot hear a Dispatcher call.

4. Recommended Protocol/Standard:

Private call usage will 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. Site access for private call is managed in the “Sites Profile Group” that the radio user belongs to.

5. Recommended Procedures:

System Managers shall work with the user groups they are responsible for to plan the appropriate private call programming requirements for those users, in order to protect the RF resources of the system.

6. Management:

The System Managers shall be 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 will be reconsidered and possibly revoked. Definition of “negative impact or excessive usage is defined as individuals who are reported for using this feature for emergency and/or non-business related matters.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.5 Sub-Section: Procedure Title: **Radio Aliases** Date Established: 12/15/06 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08-02-07

1. Purpose or Objective:

The purpose of this section is to set forth the principle by which all radio users in the regional system will establish names for their radios in order to ensure that there are no duplicate names, and also to facilitate intuitive understanding of the radio name.

2. Technical Background:

- Constraints

Every Radio User ID in the system has to be unique; there can be no duplicate IDs. The Radio User Alias field itself will hold up to 14 characters and the legal values that the system will accept are: Upper Case Alpha, Numeric, Period, Dash, Forward slash, Number sign.

When agencies make additions, deletions and changes to the database for Radio Aliases the modifications will not take affect until Motorola performs a database back-up that will occur every Friday. The Dispatch consoles will not reflect these modifications until that step is taken.

3. Operational Context:

With the exception of the first three (3) characters users are technically free to choose any unique name they wish for their radio aliases. However, since this is a shared system Radio User Aliases that are programmed into the system must have naming conventions between agencies that will not conflict with each other.

4. Recommended Protocol/Standard:

In order to meet this need the Radio User aliases would be prefixed with an agency identification that would be unique to that agency and would preferably readily identify the agency the Radio User is associated with. Because of the number of agencies using the system the prefix would be a minimum of two

alphanumeric characters in length in order to avoid contention between agencies.

Regional Operating Agencies and all agencies within the County of Broward would have naming prefixes of at least two digits that would stand alone. Counties would be pre-named with a two digit mnemonic, and the Cities and Agencies of the Counties would be included under the prefix of the County they are in.

Region 7 Operating Agencies and Broward County Region Agencies will have a naming prefix of at least two (2) letters that would describe their area. The naming standard only governs the first two characters; the characters following the first two are at the individual agency's discretion, for example; the agency may opt to internally use more than two characters for the internal identifications.

The following are suggestions for the body of the subscriber alias name. The body of the alias would contain an agency's identification for the individual or pool radio etc., possibly the radio user's call sign as an example. The alias could be suffixed with identification for the radio itself, such as a "-P" for portable for example to differentiate between a mobile & portable radio used by the same person. This would allow Dispatchers & System Managers to readily identify radio users and if the radio is a portable or a mobile.

Lost radios or radio IDs that are not associated with a radio user or console: A possibility for locating unused radios in the system that are lost, or not assigned to subscribers would be to temporarily prefix the radio serial number with a dash "-"at the time the radio is lost, or when the radio user is assigned to another radio. A report of these radios can be created by the SmartZone configuration reports tool and setting the radio selection criteria to "Radio Serial #," Start range -0, End range -999999.

A master list of Radio User Aliases will be created and maintained in the system. They will be readily accessible through the data terminal for all who have rights on that part of the system. As alias names are created and approved they will be placed on this master list so as to be available for all appropriate parties for operations and planning.

REGIONAL SYSTEM NAMING PREFIXES

2-3 Character Prefix	Name of the Agency using the Prefix
BC	Broward County Local Government
BCP	NPSPAC Mutual Aid
BCSB	Broward County CITY
BSO	Broward COUNTY's Office Police and Fire Rescue
CC	Coconut Creek
CM	Communications – Joint Operations
CS	Coral Springs
DV	Davie
DB	Deerfield Beach Fire Rescue
DN	Dania Beach Fire Rescue
FL	Fort Lauderdale
FSO	Motorola Field Service Operation (FSO)
HB	Hallandale
HBB	Hillsboro Beach
HW	Hollywood Police, Fire Rescue and Local Government
LH	Lauderhill
LP	Lighthouse Point
MED	Broward County MEDCOM
MG	Margate
MM	Miramar
OP	Oakland Park
PB	Pompano Beach Local Government
PB	Pompano Beach Fire Rescue
PL	Plantation
PP	Pembroke Pines
SEM	Seminole Tribe
SN	Sunrise
WM	Wilton Manors

5. <u>Recommended Procedures</u>:

N/A

6. <u>Management</u>:

The System Managers are responsible for seeing that the defined standard is followed and maintained.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.6 Sub-Section: Procedure Title: **Radio Model and Features** Date Established: 01/04/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

The purpose of this section is to set forth the recommended standards by which all 800 MHz radio users in the regional system will agree to purchase subscriber radios that are defined in this standard. This standard is to ensure that radios that are not in compliance do not affect the radio system. This document will be revised after the RPSCC approves the purchase and implementation of a new APCO P25 700 MHz radio system and the manufactured radio models have been identified to work with the P25 system.

2. Technical Background:

- **Constraints**

Radios must meet the recommended standards as set forth. These standards identify the proper radio to be used in conjunction with the required features and auxiliary equipment (to be described in Section 1.7) Each subscriber radio will be assigned it's unique Radio ID number, Alias Name and programmed with a codeplug/template that has been approved by the user's upper level management.

3. Operational Context:

All radios are programmed with the required Talk Groups, Mutual Aid (Local and Statewide) and features to allow it to operate on the 800 MHz Trunked radio system. Codeplugs/templates are created by the individual agencies radio shop or their contracted vendor.

4. Recommended Protocol/Standard:

In order to meet these requirements the following information describes the minimum standards that must be considered when new radios are purchased. Radios of various manufacturers and models are capable of operating on this network. The Network currently consists of a Motorola SmartZone 3600 Baud

Control Channel infrastructure. It is recommended that mobiles and portables be capable of operation with SmartZone features to permit the automatic roaming between sites as the users move out of range of their home system. SmartNet radios can be utilized where there is no intention of providing the automatic roaming features. With an eye to the future, where P25 and 700 MHz may be introduced, it is recommended that the subscriber units with a life expectancy past 2009 be either upgradeable or be equipped to operate on 700 MHz using the P25 protocol. For Public Safety users it is strongly recommended that the current Motorola products be utilized. System Managers can advise on the appropriate features, functionality and options to purchase. As a minimum, all radios shall have the ability to be assigned a unique individual ID number for system access, have the ability to be inhibited by command from the System Management tools and have an adequate talkgroup/channel capacity to permit the Local, Regional and National Mutual Aid talkgroups and channels to be programmed along with local agency requirements. The radios shall be capable of operating both in conventional mode and Motorola Trunking modes. There are other Trunking protocols that are not compatible, and radios utilizing these protocols shall not be authorized. These protocols include, but may not be limited to, Privacy Plus, EDACS, LTR and TETRA.

Mobile Radios shall have their power set to the lowest possible value. The radio systems in Broward County are designed to work in-building with portable radios. Constraints are placed upon the acceptable mobile radio power levels that should be utilized by this in-building design and the close spacing of the frequencies utilized by the network. Excessive power can cause undesired interference to the other users on the network. Older model radios shall be set to the lowest power permitted by their design, typically the half-power point. Non-Public Safety mobiles shall utilize 1/4 wave antennas, not gain style antennas.

Any Public Safety user that desires to utilize a high power setting for a specific System's Talk Groups shall obtain permission from the System Managers. The radios shall be programmed to power up in the low power mode and require a positive action on the part of the user to increase the power level. There shall be policies and procedures written to address the use of high power only after communications are unsuccessful when using the low power setting, and when working outside the primary coverage area of the network. If wide area talkgroups are involved, the totality of the wide area coverage, and not that of a more restricted coverage system, shall determine if high power usage is appropriate.

PORTABLE RADIO STANDARDS							
Model Description	**XTS2500 Model I**	**XTS2500 Model II**	**XTS2500 Model III**	**XTS5000 Model 1**	**XTS5000 Model II**	**XTS5000 Model III**	**XTS1500 Model I**
Digital	O	O	O	O	O	O	O
SmartZone	O	O	O	O	O	O	O

Dual Mode 800/700 MHz capable	S	S	S	S	S	S	S
Project 25 9600 SW	O	O	O	O	O	O	O
RF Switch (764-806 MHz) (808-870 MHz)	S	S	S	S	S	S	S
Encryption Software	O	O	O	O	O	O	
Encryption Hardware	O	O	O	O	O	O	
Multi-Key (Required only if other System Talk Groups are programmed in the radio)	O	O	O	O	O	O	

MOBILE RADIO STANDARDS			
Model Description	**XTL1500**	**XTL2500**	**XTL5000**
Digital		O	O
Dual Mode 800/700 MHz capable	S	S	S
SmartZone		O	O
P25 9600 Software	O	O	O
ID Display		O	O
Encryption Software	O	O	O
Encryption Hardware		O	O
Multi Key (Required only if other System Talk Groups are programmed in the radio)		O	O
Remote Control Head		O	O

S = Standard Feature
O = Optional Feature

5. Recommended Procedures:

N/A

6. Management:

The System Managers are responsible for seeing that the defined standard is followed and maintained.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.7 Sub-Section: Procedure Title: **Radio Auxiliary Equipment** Date Established: 01/04/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

The purpose of this section is to set forth the recommended standards by which all 800 MHz radio users in the regional system will agree to purchase subscriber radios auxiliary equipment that are defined in this standard. This standard is to ensure that radios that are not in compliance do not affect the radio system. These standards will be revised once the RPSCC has purchased and implemented a new APCO P25 700 MHz radio system and the radio model types have been identified to work with the P25 radio system.

2. Technical Background:

- **Constraints**

Radios must meet the recommended standards as set forth when auxiliary equipment is needed by the individual radio subscriber to perform their job. These standards identify the proper radio auxiliary equipment to be used in conjunction with the radio subscriber's model type.

3. Operational Context:

All radios must meet these specific requirements for antennas and batteries when installed on a subscriber's radio. Failure to utilize the manufacturer's recommended standards for the radio auxiliary equipment may cause Law Enforcement and/or Fire Rescue field force personnel to experience static, interference or audio communication breakdown with their assigned Dispatchers. While it is recognized that it is desirable to utilize the accessories manufactured by the radio manufacturer, there are alternative after-market accessories that provide performance equivalent to the manufacture's items, or functionality not available from the Original Equipment Manufacturer (OEM). The permissibility of these after-market items shall be determined by the System Manager after performing a technical evaluation to insure a performance level equivalent to the OEM items.

4. Recommended Protocol/Standard:

In order to meet these requirements the following information describes the minimum standards that must be considered when new auxiliary radio equipment is purchased.

Antennas: Radio antennas shall be either the OEM part or an equivalent as determined by the System Manager. No antenna shall be used that is not pre-approved. In no cases shall "cellular" or shortened stubby designs be permitted unless technical testing confirms that the radiated energy is within 1 dB of the OEM antenna radiation. Testing shall be performed under the direction of the System Manager, not the end user.

Batteries: The battery is the life-blood for the radio and can have a major impact on the radio performance over the course of a shift. It is encouraged that each Public Safety user will have a spare charged battery available. In car charges are an option, either the OEM version or the AdvanceTec model as appropriate for the radio model in use. These shall only be utilized to charge the spare battery. It is highly encouraged that OEM batteries be utilized as they have proven to present fewer quality and performance issues then many of the after-market products.

After-market batteries shall be evaluated prior to implementing their use. Testing shall include fit and finish, drop tests, vibration, cycle capacity, long-term capacity and self-discharge after the battery has been in use for six (6) months. Testing shall be on a representative sample of the after-market manufacturer's product.

Speaker/Microphones: Speaker/Microphones come in two basic styles; Public Safety – equipped with an antenna; Standard – usually equipped with a coiled cord and does not have antenna. The radio system coverage is predicated upon the use of a Public Safety microphone with the appropriate antenna installed on the microphone. Use of Standard speaker/microphones for users that ride in vehicles is discouraged due to the significant range reduction caused by having the antenna below the vehicle glass level and shielded by the vehicle's construction. They may be utilized by bicycle and motorcycle units with the understanding that when radio user is in a vehicle, the coverage may be significantly reduced.

Surveillance kits such as the two or three wire kits, and ComPorts also utilize the antenna mounted on the radio. The same in vehicle coverage issues apply to these units.

After-market microphones, surveillance kits, etc. require technical evaluation by the System Manager before they are promoted to the end users.

The following are the manufacturer's recommend standard specific to radio

models MTS2000 (antennas only), XTS3000 and XTS5000 (batteries only) series.

Antenna:

- 806 – 870 MHz – ½" Wavelength Whip (MTS2000 only)
- 806 – 941 MHz – ¼" Wavelength Whip (MTS2000 only)

Public Safety Microphone (Models MTS2000, XTS3000 and XTS5000):

- Straight Cable 30 inches
- Straight Cable 24 inches
- Straight Cable 18 inches
- Command Shoulder Speaker (water-proof) microphone

Batteries for Portable Radios (Models MTS2000, XTS3000 and XTS5000):

- Nickel-Cadmium 7.5 volt Battery (MTS2000)
- Ultra-High Capacity Battery (MTS2000)
- High Capacity NiCD
- High Capacity NiCD FM
- High Capacity NiMH
- High Capacity NiMH FM
- High Capacity NiMH Rugged FM
- High Capacity Lithium Ion
- NiCAD (State approved)

5. Recommended Procedures:

All Antennas, Public Safety Shoulder Mics and Batteries must meet the specifications identified in this standard, protocol and procedures. It is strongly recommended that all after-market vendors work through the System Managers to present their products for evaluation before they contact the end users. End users shall refer all vendors to their System Manager before entertaining the use of an after-market product that connects to, attaches to, or otherwise involves the subscriber units and/or the radio system.

6. Management:

The System Managers are responsible for seeing that the defined standard is followed and maintained.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.8 Sub-Section: Procedure Title: **Talk Group Names** Date Established: 01/04/07 Replaces Document Dated: 08/02/07 Date Revised: 04/08/08	RPSCC Radio Sub-Committee Approved Date: 04/08/08

1. Purpose or Objective:

The purpose of this section is to set forth the principals by which all radio users in the regional system will establish names for **Talk Groups (TG)** and to facilitate intuitive understanding of the TG name. The TG naming standard is also essential because, in keeping with the regional interoperability concept, some TG's will be shared by multiple agencies.

2. Technical Background:

All TG names programmed in the County's 800MHz Trunked Radio System must be unique and consistent from Zone Manager to subscriber. Due to the fact that the newer subscriber units will have a maximum of twelve (12) characters on their display, TG length will be limited to a maximum of twelve (12) characters. When possible, subscriber TG will be consistent with the console database and zone controller. Any subscriber with less than eight (8) characters display will be handled on a case by case basis.

3. Operational Context:

With the exception of the first four (4) characters (see Appendix A), the System Managers are technically free to choose any unique name they wish for TG's assigned within their partition (maximum of twelve (12) characters). The NPSPAC Mutual Aid conventional TG's are assigned a name that is known nationwide. When possible, subscriber TG will be consistent with the console database and zone controller. Any subscriber with less than eight (8) characters display will be handled on a case by case basis.

4. Recommended Protocol/Standard:

The first two characters of the TG alias identify the talk group governing entity/municipality (see Table 1). The third character identifies the department/agency within the governing entity/municipality (see Table 2). The fourth character will have a dash (-) as a separator. The remaining available

characters will be used to complete the talk group alias. It is important to note, depending on the subscriber type and/or model, character display may be smaller or larger. Subscribers units with displays smaller than twelve (12) characters will require condensing the TG name to fit within the display. Any subscriber displays that are under eight (8) characters will be handled, by the Radio System Administrator, on a case by case basis.

It is understood that there is currently a wide variety of subscribers out in the field. In addition to this, there are many agencies who still wish to continue to identify zone and channel assignments prior to the TG in the subscriber unit. Even though the concept that the TG's are to remain consistent from zone controller up to the subscriber is fully supported by Broward County Office of Communications Technology, this may be too big of a challenge to overcome at this time. We have come to the understanding that if the agency wishes to continue to identify zone and channel assignment prior to the TG name in the subscriber, they have this ability if they can leave the TG name consistent, as it appears in the zone controller, as much as possible.

5. Recommended Procedures:

N/A

6. Management:

The System Managers are responsible for seeing that the defined standard is followed and maintained.

Appendix A

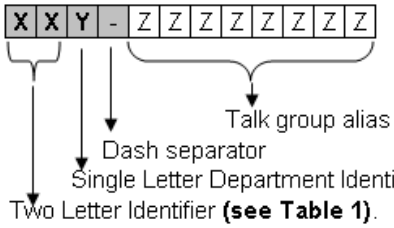
Purpose:

The following is required in order to standardize and document talk group naming convention for the Broward County SmartZone 800Mhz Trunked Radio System.

Description:

The first two characters of the talk group alias identifies the talk group governing entity/municipality. The third character identifies the department/agency within the governing entity/municipality. The fourth character will have a dash (-) as a separator. The remaining available characters will be used to complete the talk group alias. It is important to note, depending on the subscriber model, character display may be smaller or larger. Any subscriber displays that are under eight (8) characters will be handled, by the Radio System Administrator, on a case by case basis. See examples below.

Example 12 character display

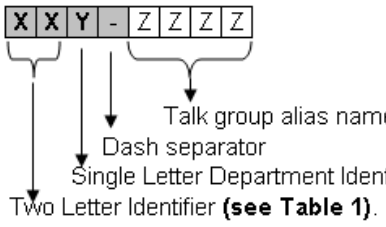


example: **B S 0** - D I S P - 4 A = PSB/BSO dispatch channel "Disp4A"

example: **F L P** - D I S T - 1 = FTL dispatch channel "Dist-1"

Note: Depending on the subscriber model, character display may be smaller or larger. There is a max of twelve (12) characters allowed for talk group alias names.

Example 8 character display



example: **B S 0** - D S P 4 = PSB/BSO dispatch channel "Disp4A"

example: **F L P** - D S T 1 = FTL dispatch channel "Dist-1"

Note: Depending on the subscriber model, character display may be smaller or larger. There is a max of twelve (12)

Tables

Table 1	
BC	Broward County
BS	Broward Sheriff Office
CC	Cooper City
CK	Coconut Creek
CS	Coral Springs
DN	Dania
DR	Deerfield
DV	Davie
FL	Fort Lauderdale
HA	Hialeah, Miami Dade Cty.
HD	Hallandale
HW	Hollywood
LH	Lauderhill
LL	Lauderdale Lakes
LP	Lighthouse Point
LS	Lauderdale by the Sea
LZ	Lazy Lake
MC	City of Miami, Miami Dade Cty.
MB	Miami Beach, Miami Dade Cty.
MD	Miami-Dade County
MG	Margate
MM	Miramar
NL	North Lauderdale
OP	Oakland Park
PC	Palm Beach County
PB	Pompano Beach
PD	Parkland
PK	Pembroke Park
PL	Plantation
PP	Pembroke Pines
SF	State of Florida
SM	Seminole
SN	Sunrise
SR	Sea Ranch Lakes
SW	Southwest Ranches
TM	Tamarac
WM	Wilton Manors
WP	West Park
WS	Weston

Table 2	
A	**Airport**
B	FUTURE USE
C	**Communications**
D	FUTURE USE
E	**Port Everglades**
F	**Fire Rescue**
G	FUTURE USE
H	FUTURE USE
I	FUTURE USE
J	FUTURE USE
K	FUTURE USE
L	**Local Government**
M	**Mutual Aide**
N	FUTURE USE
O	Office*
P	**Police**
Q	FUTURE USE
R	**Parks & Rec**
S	**School**
T	FUTURE USE
U	FUTURE USE
V	FUTURE USE
W	FUTURE USE
X	FUTURE USE
Y	FUTURE USE
Z	FUTURE USE

*** To be used only by Broward Sheriff's Office**

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.9 Sub-Section: Procedure Title: **Shared Use Of Talk Groups** Date Established: 01/04/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

The intent of this standard is to provide an option to the users of the 800 MHz system, which will allow the talk group owners to "at their discretion" predefine sharing authorizations for other agencies.

2. Operational Context:

Talk Groups are considered to be "Owned" by the agency requesting the creation of the Talk Group, similar to the ownership that applies to conventional RF resources. As the owner of the Talk Group the owning agency has the authority and control to define who can and cannot use the Talk Group and to what "degree. Traditionally this process has been primarily accomplished with "letters of authorization."

The optional method to simplify this process is for the owning agency to predefine sharing authorization, as diagrammed in the table example below.

The predefined authorizations would be kept in the Talk Group spreadsheet maintained by the System Managers. These spreadsheets would be shared between the System Managers, and would be a reference available for Talk Group planning. If an agency does not pre-define sharing authorization for a particular talk group, the default will be a "P" as defined below.

3. Recommended Protocol/Standard:

The use of the following codes, which are combined to define the intended pre-authorizations…

P = Permission is required to gain authorization for use. A letter of permission must be generated from the System Manager of that agency that wishes to use another agency's Talk Groups for their radio subscribers and/or their Dispatch consoles and this written request must

be sent to the System Manager of the system that has ownership of those Talk Groups for their system.

D = Defined agencies may share, to be defined in a separate letter. The letter would outline specific purpose talk groups, i.e., only dispatch consoles, only neighboring cities, etc. The letter will be on file with the appropriate System Managers.

L = Like agencies may share, "Fire, Medical, Law, Public Works, etc."

A = All agencies.

RX = Only authorized to receive.

TX = Authorized to transmit and receive.

4. Recommended Procedures:

The System Managers, working with the user groups, would perform this task.

5. Management:

The System Managers are responsible for the management of this procedure. The larger table is also used to layout the Fleetmap information as described in this manual in Section 1.1, Fleetmap Standards.

Talk Group	Owning Agency	Description	Administrating Agency	Global Sharing Authorizations P = Permission letter required to gain authorization for use D = Defined Use – Letter required L = Like agencies may share "Fire, Medical, Law, Works" etc. A = All agencies RX = Are only authorized to receive TX = Are authorized to receive & transmit
Talk Group 1				D-TX
Talk Group 2				L-TX
Talk Group 3				A-TX
Talk Group 4				P-RX
Talk Group 5				P-TX
Talk Group 6				D-TX
Talk Group 7				L-TX
Talk Group 8				A-TX

Talk Group 9				P-RX
Talk Group 10				P-TX
Talk Group 11				D-TX
Talk Group 12				L-TX
Talk Group 13				A-RX
Talk Group 14				P-RX
Etc.				P-RX

The “RX” option shown in the table is an authorization that permits receive only use, although the radio would be technically capable of transmit (TX) operation on the talk group.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.10 Sub-Section: Procedure Title: **Scanning Talk Groups** Date Established: 01/04/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

This procedure is to identify operational procedures and responsible authorities governing Scanning activities as it relates to the Scan function in the individual subscriber radio.

2. Technical Background:

- **Capabilities**

  The network infrastructure and subscriber units need to be configured to permit managed user Scanning of Talk Groups. Whether or not Scanning will be utilized in subscriber radios, it is at the option of the user agency. Users also need to be trained that merely including a Talk Group in a non-priority Scan list will not necessarily result in the user hearing traffic on that Talk Group. The Talk Group must also be "active" at the site where the user is affiliated. Talk Groups are active on a site if the Zone Controller is programmed to allow the Talk Group to appear on that site and there is at least one user affiliated at the site which has the Talk Group of interest as their selected channel.

- **Constraints**

  How the radio is programmed to handle wide area and local sub-system Talk Groups will determine priority Scan capabilities. If the local sub-system Talk Groups is not programmed to the same "system" in the radio, they cannot be included in the priority monitor Scan list. In this case, only Talk Group Scan can be implemented. Priority Scan requires System Infrastructure configuration in order to perform as expected. The Talk Groups that are deemed to be Priority Monitor Groups need to be configured as such by the System Managers. There are practical limitations on the overall number of Priority Monitor Groups that can be enabled due to the amount of time required to distribute the list of active Talk Groups to the radios in real-time. Talk Group Scan does not provide

a priority feature to direct the radio to the priority Talk Group. Talk Group Scan can Scan Talk Groups from different systems (as defined in the radio internal programming) and conventional channels. It is strongly recommended that "talkback Scan" not be used. Talkback Scan would direct the user to transmit on the last active Talk Group the radio heard traffic on. This will cause confusion as the radio user will not know what Talk Group the radio will be transmitting on as it will constantly change based upon what the radio last received. Scan is not recommended for those users that must hear critical communications.

While Scanning will be available on the systems it will necessarily be limited and, therefore, not be as robust as in conventional radio systems.

3. Operational Context:

The network infrastructure and subscriber units will be configured to balance the ability for users to achieve wide area coverage where necessary, and maintain an acceptable level of service for all users. The use of "Critical User" and "Critical Site" in the system for the purpose of non-priority Scanning is not permitted and Scanning between different sites will be accomplished by the use of "requested sites."

Before priority Scanning is allowed on an individual subscriber's radio, it must be pre-approved by the agency's management and/or command.

Additionally, priority Scanning of Talk Groups must be evaluated by the System Manager to make sure the radio system is not affected by the use of this feature.

4. Recommended Protocol/Standard:

Limited Scanning/monitoring privileges may be pre approved by the affected Talk Group owners and System Managers.

Before Scanning of owned Talk Groups, permission must be granted. permission must come from:

- The System Managers of the sites that are being requested for the Talk Group
- The jurisdiction/agency who is the "owner" of the requested Talk Group

Mutual aid, special roaming and other shared Talk Groups may be Scanned at any time; however, "requested site" determinations will be made by the System Managers of the affected sites.

5. Recommended Procedures:

Permission:
If the Talk Group does not appear on the approved Scanning list, permission must be obtained in writing from the Talk Group owner and the System Manager of the non-home site or sites being "requested" if applicable.

Scanning Configuration:
If trunked Scanning is desired, it is recommended that Scanning should normally be limited to owned trunked Talk Groups which are affiliated with their "always preferred site(s)".

It is further recommended that Scanning normally be disabled when the user leaves the system and switches their radio to a conventional (non-trunked) channel. However, if mixed mode Scanning (both trunked Talk Groups and conventional channel members) is required by some users, it is also recommended that this Scan type only be available when the radio is selected to a conventional channel. This is because mixed mode Scan does not provide priority reverts and the user will typically miss substantial portions of conversations on the selected channel. Talkback Scan is highly discouraged, as the user cannot control the Talk Group used to transmit. Can lists can be either programmed into the radio with no user access for changes, or the list can be made accessible for user modifications. It is preferred that the list is made user configurable to allow those users that can handle Scan to determine what they want to listen to and make changes "on the fly" as their requirements change.

Scanning of Non Home Site Talk Groups:

It is possible to monitor a non home Talk Group by configuring the system to request the desired non home Talk Group appears on your primary/home system or "always preferred site(s)". Doing so however, will consume a repeater channel on your primary/home system or "always preferred site(s)" and will carry the requested non-home Talk Group priority setting with it. Also, a call on the requested non-home Talk Group will not be delayed (busy queued) if the home system or "always preferred site(s)" does not have a channel available. This however may cause unacceptable conditions where the majority of users do not receive the call while the dispatcher or calling party has no indication that a large segment of their users did not receive the call. While this "requested site" is the recommended approach, it must be carefully controlled, monitored and evaluated due to the potential to exhaust system resources. It must be approved by the affected System Managers.

6. Management:

The System Managers will be the final authority for controlling the Scan feature and Scanning issues. The agency's management and/or command will have the authority to approve/disapprove this feature for their users.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.11 Sub-Section: Procedure Title: **Emergency Button** Date Established: 01/04/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

There will be a large variety of users on the radio system with various Emergency Button needs. The various ways the emergency key can be configured will allow for flexibility of use, however, it is important to design the system in such a way that when an Emergency Button is pushed, it is responded to quickly and appropriately.

2. Technical Background:

- **Capabilities**

  The "Emergency Button" feature, if it is programmed into the subscribing agency radios, will allow a radio user to send an emergency notification by pressing the specific Emergency Button on the radio. The notifications will audibly and visually alert all dispatch console positions that have the talk group up that the emergency notification is routed to. Other radios that have the talk group selected will also receive the emergency notification, and display the radio ID of the radio generating the emergency. The display of an ID is dependent upon radio model, firmware version, and purchased options. The user activating the Emergency Button has the obligation to properly cancel the activation by pushing – and holding the Emergency Button until a continuous tone sounds. Failure to properly cancel the alarm on the originating radio will cause a new alarm activation each time the user transmits.

  Emergency calls are also automatically assigned the highest priority available and would be the first available from the queue if the system is in a busy situation. Subscriber's radios can optionally be configured to automatically activate the Push-to-Talk (PTT) for a programmed period of time if the Emergency Button is pressed.

- **Constraints**

  Consider two situations a fire department engine company could be faced with, that show different operational needs:

  1. An engine company responds to a medical at a private home. Upon entering the home, they are met by an out-of-control person who fires a handgun at them.

  2. An engine company is conducting an interior fire attack when the floor collapses, trapping them in the basement.

  In the first example, a firefighter may push his Emergency Button as he is running out of the home. He may want it to signal his dispatcher on the main talk group. The dispatcher would immediately see the signal, assess the situation, and send the police to assist.

  In the second example, a firefighter may push his Emergency Button, and have it send the signal on his fire ground operations channel. The on-scene safety officer would attend to this signal by immediately sending in a rescue crew comprised of people already at the scene.

  The design should also avoid the instance where an Emergency Button is pressed, and nobody can identify the user, or the wrong people attend to the emergency. Such a situation would occur if a police officer's Emergency Button were configured to signal on a Main Channel talk group. In that case, pressing his Emergency Button would probably signal every police dispatch console on the radio system.

  Another example is that a public health official pushing the button when alone in a dangerous situation. If the public health official's radio were configured to signal on the County COUNTY main dispatch talk group, but is unknown to the dispatcher, the dispatcher may be confused by who is in distress, and may not know how to respond. This example shows the importance of an agreement between the central monitoring agency and the radio user agency.

  Emergency Button programming cannot be configured on a talk group by talk group basis. This function is defined within the radio personality consisting of a group of 15 talk groups. The personality may be configured to direct the radio to a specific talk group or to use the current selected talk group of the talk groups within the personality. Emergency Button configuration requests shall be discussed with the System Manager of the affected System as radio programming codeplugs are impacted.

It is recommended that non-Public safety, i.e. Public Service, or general government, users not have the Emergency Button functionality unless appropriate training and monitoring resources are available to respond to the alarms. Non-public safety emergency alarms shall not be directed to a Public Safety Talk Group unless the Public Safety Dispatch Center responsible for the Talk Group agrees to assume responsibility for the alarms.

3. Operational Context:

An Agency may choose to utilize the Emergency Button functionality, or to disable its use. If an Agency chooses to use the Emergency Button it shall be utilized as an indication of an immediate threat to life or property. Use of the Emergency Button to advance a routine Talk Group call in the priority cue is not an accepted usage. Agencies may choose to have the emergency activations occur on a primary dispatch Talk Group, or be directed to a specific Talk Group set aside to handle Emergency Activations. Agencies that may have access to the Talk Groups from other Agencies in their consoles will receive the emergency activation notifications if that Talk Group is active in a folder in the console operator position. Agencies shall NOT acknowledge/silence/cancel emergency activations from another Agency without contacting that agency before taking action. To do so may cause a valid emergency alarm to go unanswered.

Any Agency that acknowledges/silences/cancels emergency activations from another Agency more than 3 times, without contacting that agency before taking action, shall remove the other Agency Talk Groups from their consoles within 30 days of receiving notification from the Talk Group owner or System Manager.

Subscriber units that send an excessive number of false emergency alarm activations shall be located and corrected by the subscriber owner agency as expediently as possible. Excessive is determined to be four (4) or more false alarm activations within a 24-hour period. The subscriber owner agency shall take all steps necessary to locate and correct the false activations. There are circumstances where it is not possible to stop the false activations by attempting to inhibit the radio or by removing the radio authorization record from the system databases. In these cases the radio must and shall be located by the Owner Agency and brought to the servicing vendor for repairs within 30 days of the first false activation. Dispatch Centers shall report all instances of excessive false emergency alarm activation to their System Manager. The report shall include the date, time and Talk Group the emergency occurred on, along with either the subscriber alias or displayed radio ID #.

4. Recommended Protocol/Standard:

Use of the Emergency Button as an emergency signaling option should be available to any agency on the radio system, subject to certain conditions and

provisions.

1. Agencies are not required to use this capability of the radio system.
2. No agency will be permitted to enable their emergency signal on a talk group designated as “emergency restricted.”
3. All agencies implementing the Emergency Button must have a plan in place to respond to an Emergency Button activation.
4. All Emergency Button response plans must include, at minimum:
    - A central radio monitoring point that can identify which radio user pushed the button, the location and nature of the emergency and what the proper agency response should be
    - A central monitoring point must be available during any/all hours that personnel are using the radio system.
    - A policy for use of the Emergency Button by radio users.
    - A response plan 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 must be in place among the agencies.
    - Where available the orange button should be used to program the Emergency Button.

5. Recommended Procedures:

N/A

6. Management:

Agencies wishing to use the Emergency Button function must coordinate which agency resources that will be receiving the emergency calls, the receiving agencies must have an appropriate plan in place, and documented as to the process that they will use to handle the emergency calls.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.12 Sub-Section: Procedure Title: **Encryption** Date Established: 01/04/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

This procedure is to identify operational procedures and responsible authorities governing Encryption activities.

2. Technical Background:

- **Capabilities**

  The network infrastructure and subscriber units need to be configured to permit Encryption of selected Talk Groups. Whether or not Encryption will be utilized in subscriber radios, it is at the option of the user agency. Users also need to be trained to know how to activate the Encryption feature when needed on a specified talk group.

- **Constraints**

  It will be the subscriber radio user's responsibility to activate the Encryption feature when needed. In most cases the use of Encryption will be decided once a talk group is dedicated to the use by the personnel in the field that are involved in the operational situation.

  The Encryption feature blocks all non-approved/intruder radio users and scanners from hearing the conversation of the talk group that is being used for the situation. At this point in time (2007), only the City of Hollywood and County of Broward infrastructure support Encryption capabilities. Encryption can only occur on a digital capable talk group. Both the availability of digital Talk Groups and digital subscriber IDs is limited and must be coordinated with the System Managers prior to any desired implementation. Currently only DES-OFB and DES-XL Encryption algorithms are supported. Encryption Talk Groups that must appear on a console will need to have Encryption key loaded into the Console DIU. This has the potential to reduce the security of the talk group as others may be able to access the clear audio via a console.

3. Operational Context:

The Encryption feature needs to be pre approved by the agency's upper level management. Police units that are approved to receive Encryption for their subscriber radios are designated as SWAT, K-9, Homeland Security and Special Investigation Division, and any other unit as determined by the Department. Other Departments and Divisions such as the Fire Department may choose to encrypt some or all of their Talk Groups as needed to insure operational security.

4. Recommended Protocol/Standard:

Limited Encryption privileges may be pre approved by the affected Talk Group owners and System Managers.

Before allowing Encryption as a feature of a subscriber radio user of owned Talk Groups, permission must be granted. Permission must come from:

- The System Managers of the sites that are being requested for the talk group
- The jurisdiction/agency who is the "owner" of the requested talk group

5. Recommended Procedures:

A subscriber radio user that has the Encryption feature will be responsible for activating/deactivating it as needed. Talk Groups may also be "strapped" secure in the subscriber programming to permit only encrypted operation if desired.

Encryption Keys shall be maintained by the Agency utilizing the Encryption feature. Each agency is responsible to insure that they do not duplicate Logical IDs (LIDs). Logical IDs for the keys consist of a four-digit number entered as the last four digits of the Key. LIDs for Broward County shall be in the 1000 series, Deerfield Beach shall use 2000, Hollywood shall use 3000, Fort Lauderdale and Pompano Beach shall use 4000, and Hallandale Beach shall use 5000. As other systems are brought into the Regional Public Safety Communications System, their LIDs shall start with the site number for their infrastructure. This structure insures that there will not be duplicated LIDs which will cause problems when utilizing Encryption in the integrated environment that we share. The first 16 digits of the key are at the discretion of the Agency.

There are two shared Regional Special Investigations Joint Operations Talk Groups that utilize a shared common key. These two Talk Groups may not be utilized on a permanent basis for any one specific unit or agency. They are common, shared resources dedicated to interagency operations. The talk group information and key are available to authorized personnel by contacting either the System Managers of the Broward COUNTY's Office and Fort Lauderdale.

6. Management:

The System Managers group and the agencies upper level management will be the responsible authority for Encryption issues.

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.13 Sub-Section: Procedure Title: **Definitions & Acronyms** Date Established: 06/28/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

To clarify terms used throughout the standards, protocols and procedures manual. All definitions will be found in this section.

2. Management:

Should there be additions, deletions or changes to these procedures the Regional Public Safety Communications Committee (RPSCC) members are responsible for revising this section.

3. Definitions (in alphabetical order)

APCO P25 Compliant: Public safety equipment that meets (Association of Public Safety Communications Officials) APCO P25 standards.

Announcement Group: is a collection of Talk Groups.

Audit: An audit is defined as a one time, infrequent or occasional in depth analysis of comprehensive elements. An audit may be annual or upon demand. An audit may be stimulated by an event or complaint of monitoring outcome.

"Common" or "Pool" Talk Groups: Common/pooled talk groups (TG) are those that are set-aside for communicating across multiple agencies. Agency radio users in appropriate service areas who need to talk to one another for day to day business or for mutual aid will all put the appropriate common or pool talk group in their radios to be available in time of need. Example: Fire Departments will all have the common Statewide Fire Mutual Aid TG in their radios. "Pool" is distinguished from "common" in that pool implies more then one, such as TAC 1 – 4 is a pool of common regional tactical TGs for law enforcement.

Failsoft Signaling: During normal system operation, the central controller supplies the base station's Failsoft circuit with a Transmit Data (TDATA) signal. The TDATA signal consists of an OSW followed by an LSHS signal, followed by

a Disconnect Word signal. The TDATA signal keeps the base stations in the trunking mode. If TDATA transmission stops because of failure of the central controller, the base stations revert to the Failsoft mode.

- The base station unmutes and transmits a Failsoft data word
- Radios respond to the Failsoft word and unmute, allowing service to continue via community repeater type operation.
- The base station sends out a 900 Hz tone for 280 milliseconds every 10 seconds to alert the radio user that the system is in Failsoft mode.

Logging: Audio recording of a radio communication.

Mission Critical Operations: Those governmental, quasi-governmental and non-governmental operations carried out by authorized users which are reliant upon a functioning two-way radio communications system which unavailability, degradation, delay or failure, partial or complete, would significantly impact or impair the successful delivery of a vital service or mission. Operations would include, but are not limited to the categories below:

- Public Safety – Those functions of government that exist to protect the physical well being of the public as a whole from physical danger – continuous delivery of essential public services. Included with this group are Legal Counsel and CITY's Special Investigative Unit (SIU) and the Administration Site Operations.

- Transportation – Those functions of the government that exist to provide safe, effective and efficient multi-mode movement of the public commodities including public roads, highways, waterways, railways, airways and public transportation systems. Included with this section is the Broward CITY buses that may need to be used as a back-up to the Broward County Mass Transit buses should a mass evacuation occur due to a major incident.

- Environmental Protection – Those functions of the government that exist to protect the environmental from changes that are detrimental to the existence and continuance of that environment.

- Public Works – Those functions of the government that provide "first responders" that may be necessary to clear streets and highways so that Public Safety operations can be conducted after a major event like a hurricane.

Mobile Radio: A station in the mobile service, generally installed in a vehicle, intended to be used while in motion or during halts at unspecified points.

Mobile Service: A service of radio communication between mobile and base

stations, or between mobile stations.

Monitor: Monitoring is defined as the scheduled and routine inspection of operational practices and facilities and/or the review of system reports and documents. Monitoring frequency would generally be on a predetermined, scheduled basis

Non-Critical Operations: All other governmental, quasi-governmental and non-governmental operations, which are reliant upon a functioning two-way, radio communications that do not meet the above mission critical or department critical definitions.

Operational Fixed Station: A fixed station, not open to public correspondence, operated by, and for the sole use of those agencies operating their own radio communication facilities in Public Safety, Industrial, Land Transportation, Marine or Aviation Radio Services.

Patch:

Permanent (hard) Patch: A patch between two or more audio resources on a system, which is fixed and cannot be controlled or edited by the dispatcher.

Manual (soft) Patch: A patch between two or more audio resources on the system, which is setup and controlled by the dispatcher. The dispatcher owning the patch can add and delete resources as needed.

Portable Radio: A radio that is completely freestanding and may be hand-carried or worn by the radio user.

Preferred Site Assignment: A SmartZone system can also be configured with Preferred Site Assignment operation. This feature allows radio users to maintain conversations on sites especially useful to operations and group requirements. In areas with overlapping coverage, radios will work on their preferred site in order to efficiently utilize channel resources while minimizing the number of channels necessary to complete a talkgroup call. Four types of preference can be programmed into the radio personality:

- **Always Preferred –** The subscriber unit will always use this site if it has at least acceptable signal strength, even if the site enters site trunking mode.
- **Preferred -** The subscriber unit will use this site if it has at least an acceptable signal strength rating and is in wide-area trunking mode.
- **No Preferred Site –** This is the default setting for subscriber radios. The subscriber unit will use the best signal according to the best Receive Signal Strength Indication (RSSI).
- **Least Preferred –** The subscriber unit will avoid this site unless no other sites with at least acceptable signal strength are available for use.

Private Call: This allows one radio user to talk to and be heard by only one other radio user. This feature allows a supervisor to discuss confidential matters with a particular member of a talkgroup while other members of the same talkgroup remain squelched.

Public Safety: All Law Enforcement / COUNTY, Fire, Emergency Medical and related service areas. These include badged and/or sworn ancillary personnel such as Park Rangers, Court Security Officers, Community Corrections, and those who support public safety operations under special circumstances.

Public Safety Answering Points (PSAPs):

Primary: The PSAP where a 9-1-1 call is originated and received by a call taker then transferred to a dispatcher for dispatching police, fire or emergency medical assistance.

Secondary: The PSAP that receives transferred 9-1-1 call taker calls and is then dispatched and monitored from this center.

Public Service: Public Service in this context refers to general government personnel such as Public Works, Transportation, and other similar public service operations.

RF: Radio Frequencies

Regional Public Safety Communications Committee (RPSCC): The governing body of municipal Police and Fire Chief's, IT Management and decision-making staff that are empowered to develop Standards, Protocols and Procedures regarding the intent to accomplish the Broward County's Charter direction to achieve regional communication plans to establish Radio Interoperability and Closest User Response objectives.

Region 7: State of Florida Homeland Security region that is made up of Broward, Dade, Monroe and Palm Beach Counties.

Regional System: In this context of this manual this term is intended to represent the entire Region-wide 800 MHz Public Safety Communication System.

SmartZone Trunked System: The 28 channel trunked radio system that serves public safety communication users in a wide-area coverage network. This system allows for roaming from one radio system to another trunked or conventional system seamlessly and provides communications back to the municipality's home based dispatch center. This system can operate in an analog or digital mode.

SmartZone Manager Terminal: The resource tool that is used by System Managers to administer their radio system for maintenance issues and controls of how their radio subscriber and consoles are configured / programmed.

Subscriber Radio: A portable radio that is assigned to a specific individual or a mobile radio that is shared by multiple staff that drives and operates the vehicle.

System: A countywide public safety radio communication system that consists of a shared region-wide infrastructure, the elements of which are identified in the Regional Public Safety Communications Plan and Subsystem integrated into or interconnected by the shared countywide network.

System Manager/ Administrator Positions:

- System Manager – individual in charge of the radio system of a participating agency.

- System Administrator – individual who is responsible for the day to day radio system operations of a participating agency.

- Sub-System Administrator – individual who is responsible for the day to day radio sub-system operations of a participating agency.

- Contract Manager – Director of Broward County Office of Communications Technology or his appointed designee.

Talk Group: The Talk Group is the primary level of communication in a Trunked radio system. This provides the effect of a private channel down to the talkgroup level and prevents members of one talkgroup from hearing the talkgroup calls generated by radios in other talkgroups.

Telephone Interconnect: The use of a radio to make a two-way call between two radios subscribers when privacy is needed to block other radio subscribers from hearing the conversation. This feature must be programmed in the radio and activated on the system in order for it to be functional.

Variance: An allowed divergence from full adherence of an adopted standard, protocol or procedures

Waiver: A complete release from an adopted standard, protocol or procedure.

4. **ACRONYMS (in alphabetical order)**

ALS - Advanced Life Support

ATAC	-	All (user) Tactical talk group for 800 radios
AVL	-	Automatic Vehicle Locator
APCO	-	Associated Public Safety Communications Officials
BLS	-	Basic Life Support
CEB	-	Central Electronics Bank
CTCSS	-	Continuous Tone Coded Squelch System
DIU	-	Digital Interface Unit
DTMF	-	Dual Tone Multiple frequency
EDICS		Emergency Deployable Interoperability Communications System
EMS	-	Emergency Medical Services
EMRS	-	Emergency Medical Radio System
FCC	-	Federal Communications Commission
ICALL	-	International 800 MHz Calling Channel
ITAC	-	International 800 MHz Tactical Channel
MHz	-	Megahertz
NAEMSD	-	National Association of State EMS Directors
NPSPAC		National Public Safety Planning Advisory Committee
PSAP	-	Public Safety Answering Point
PSWAN		Public Safety Wide Area Network
PTT	-	Push to Talk, i.e. talk button
RF	-	Radio Frequency
RX	-	Receiver of radio communications
SMG	-	System Manager, the owner of the Regional Public

		Radio System and Sub-Systems
RSS	-	Radio Service Software
TX	-	Transmission of radio communications
UHF	-	Ultra High Frequency
VHF	-	Very High Frequency

STANDARD OPERATING PROCEDURES (SOP)

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section: 1.14 Sub-Section: Procedure Title: **Console Naming** Date Established: 06/28/07 Replaces Document Dated: N/A Date Revised: N/A	RPSCC Radio Sub-Committee Approved Date: 08/02/07

1. Purpose or Objective:

The purpose of this section is to set forth the principle by which all System Managers / Administrators of the regional system will establish names for the Radio IDs used to support dispatch console positions. This is necessary because IDs are not associated with a Radio User Alias.

2. Technical Background:

Constraints: The serial number field in Radio ID screens in 12 characters long. Every Talkgroup per console position requires a Radio ID programmed for that position, for example a single console position may have 50 radio ID programmed to support that position.

3. **Operational Context:** Every radio in the system represents a radio, but not every Radio ID in the system is a radio, some are consoles. By planning an identification process, we can use the radio serial number field in the radio entry screen in the system to categorize consoles so that they can be easily identified.

4, **Recommended Protocol/Standard**: The Serial Numbers used in the records for console Operator positions will be formatted according to the following:

OPTION 1

- Regional Operating Agencies would have naming prefixes of at least two characters that would stand alone. Counties would be pre-named with a two character identifying mnemonic, and the Cities and Agencies of the Counties would be included under prefix of the County they are in.
- The next three characters would be the letters “con” for console, so as to easily distinguish this identifier from other radio aliases.
- The characters following these first five are at the individual agency’s discretion.

OPTION 2

- Starting with a 2 – digit prefix to identify the Console location “for example FL, PB, HL, etc.
- The next 2 digits represent the CEB number.
- The following 2 digits indicate the TDM slot on that CEB
- The last four characters are to be unique, at the individual agency discretion.

4. Recommended Procedures:

   N/A

5. Management:

   The System Managers / Administrators are responsible for ensuring compliance with the standard.