



---

## **TRWC Board of Directors Meeting**

Monday, September 14, 2009, 10 am to 12 pm

Location: Town of Gilbert – Room 233  
50 E. Civic Center Drive  
Gilbert, AZ 85296

### **Agenda**

#### **1. Agenda Review**

Topic Leader: Chairman Kross

#### **2. Action on the 03/30/09 TRWC Board Meeting Minutes**

Topic Leader: Chairman Kross

#### **3. Action on recommended Policies and Procedures**

Topic Leader: Executive Director & Randy Thompson

*Attachment – TRWC Policies and Procedures*

#### **4. Discussion/Possible Action on Rural Metro TRWC Interest**

Topic Leader: Executive Director

*Attachment – Rural Metro Letter*

#### **5. Update on Reconfiguration Status**

Topic Leader: Executive Director & Jeff Toye

#### **6. Update/Possible Action on IGA with (Phoenix) RWC**

Topic Leader: Executive Director

#### **7. Update/Possible Action on Data Radio System**

Topic Leader: Executive Director & John Minick

#### **8. Update/Possible Action on the Fiscal Year 08/09 & 09/10 Budget**

Topic Leader: Executive Director & Denny Fulton

*Attachments – FY 2008/2009 Recap & FY 2009/2010 Review*

*Discuss Potential Change in Cash Flow for Reconfiguration and White Tanks*

#### **9. Updates from the Executive Director**

- Gary Bradbury's Departure
- Rio Verde Status
- Shawn Woolley's Appointment
- Gila River Status
- MPS Status
- Stimulus Funding

#### **10. Meeting Summary and Next Meeting Preview**

Topic Leader: Executive Director

#### **11. Adjournment**



---

## **TRWC Board of Directors Meeting**

Monday, September 14, 2009, 10 am to 12 pm

Location: Town of Gilbert – Room 233  
50 E. Civic Center Drive  
Gilbert, AZ 85296

**Members Present:** *Mesa:* Dale Shaw (Exec. Dir.), Alex Deshuk; *Queen Creek:* John Kross; *Gilbert:* Shawn Woolley; *AJFD:* Chuck Zanella; *Apache Junction:* Kathy Jeter; *TRWC Attorney:* Bill Anger (Engelman Berger)

**Guests Present:** *Mesa:* Randy Thompson, Denny Fulton, Mike Brown, Shirl Butler, John Minick, Bruce McGregor, Brian Kotsur, *Rural/Metro Fire:* Chuck Fitzgerald, Chief, Dan Caudle, Peter Zick, *Rio Verde Fire:* Gary Bradbury, Jerry Fickes, *Phoenix Fire:* Doug Mummert, *Motorola:* Mike Sumnicht, Ricardo Aguilar, Miguel Lomba

**Recorder:** Leslie Dibble

## **Minutes**

### **Agenda Review**

Topic Leader: Chairman Kross

Chairman Kross reviewed the [agenda](#) items with the Board.

### **Action on the 03/30/09 TRWC Board Meeting Minutes**

Topic Leader: Chairman Kross

Chairman Kross asked for a motion for consideration of the 3/30/09 Board meeting [minutes](#). There was a motion to approve by Chuck Zanella and a second by Kathy Jeter. All were in favor.

### **Action on recommended Policies and Procedures**

Topic Leader: Executive Director & Randy Thompson

Dale and Randy provided a brief overview of proposed policies and procedures. The administrative manager, Mesa, moving forward along with its partners, will use these policies and procedures for operational purposes. They cover three major areas: operations/maintenance, configuration management, and network security. The TRWC Committees; Technical, Operational and Executive have all recommended approval to the Board through the Executive Director.

Chairman Kross asked for a motion for consideration of the adoption of the [Policies and Procedures](#). There was a motion to approve by Alex Deshuk and a second by Chuck Zanella. All were in favor.

### **Discussion/Possible Action on Rural Metro TRWC Interest**

Topic Leader: Executive Director

Guest Speaker: Fire Chief, Dan Caudle, of Rural Metro, and Bruce McGregor of Mesa Fire

A [letter](#) from Rural Metro was sent as a request to be considered as an Interoperability Participant with the TRWC.

The Executive Director, after conversations with Mesa Communications technical staff, stated that there does not appear to be any negative impacts to the system moving forward, if the Board agrees. Chairman Kross asked for a motion for consideration to direct the Executive Director to move forward with the development of an Interoperability agreement/contract with Rural Metro and Mesa as TRWC administrator. There was a motion to approve by Chuck Zanella and a second by Kathy Jeter. All were in favor.

#### **Update on Reconfiguration Status**

Topic Leader: Executive Director & Jeff Toye (absent)

Dale Shaw announced that we are on schedule for the first quarter of 2010. We are currently working with our vendor, Motorola, to establish a detailed timeline on the implementation of the new equipment that will establish the TRWC as an independent system, along with identifying the steps that are necessary technically to accomplish this. As of now, we are on a timeline of end of January early February to have the implementation occur to establish an independent system.

In conjunction with the reconfiguration, Dale Shaw gave an update on the White Tanks site, improving coverage on the west side. Antennas could be installed as early as the end of September and equipment put in place in October.

The only remaining item, related to reconfiguration, is establishing talkgroups for interoperability with the RWC. Discussions have gone well regarding talkgroups and we are in general agreement on approach.

#### **Update/Possible Action on IGA with (Phoenix) RWC**

Topic Leader: Executive Director

We have continued work on establishing interoperability with the RWC. We have submitted a draft IGA to Phoenix. The IGA has been operationally accepted and is now going through legal review with Phoenix, acting as the administrator of the RWC.

#### **Update/Possible Action on Data Radio System**

Topic Leader: Executive Director & John Minick (Mesa Communications)

[HPD Subscriber Equipment Pricing](#)

A [presentation on the data radio system](#) that is used by Mesa and some of the TRWC partners was presented by John Minick. An upgrade for the current system is necessary due to the system being 10 years old and obsolete. This system is used for CAD and AVL and is used by Mesa's Police and Fire, Gilbert and Queen Creek use it for their Fire dispatch. A cost breakdown and review of recovery of costs for the upgrade to those participating in the use of the system was included with the presentation. Dale Shaw will confirm the existing numbers within the next two weeks via email to participants for their budgeting use.

#### **Update/Possible Action on the Fiscal Year 08/09 & 09/10 Budget**

Topic Leader: Executive Director & Denny Fulton

[FY 2008/2009 Recap & FY 2009/2010 Review](#)

[Discuss Potential Change in Cash Flow for Reconfiguration and White Tanks](#)

After reviewing the data Denny provided, the board members agreed to be billed now instead of waiting for the 2010 billing date.

Chairman Kross asked for a motion to approve the proposed change in invoicing as presented by Denny Fulton. There was a motion to approve by Chuck Zanella and a second by Kathy Jeter. All were in favor.

## **Updates from the Executive Director**

- Gary Bradbury's Departure
  - i. Gary has retired from Mesa Fire and is now the Fire Chief for Rio Verde. The Board congratulated him on his new position.
- Rio Verde Status
  - i. The change in Rio Verde Fire leadership has caused a renewal of interest in establishing a formal arrangement with the TRWC
- Shawn Woolley's Appointment
  - i. Shawn has accepted the chair position of the TRWC Executive Committee due to the retirement of Chief Bradbury
- Gila River Status
  - i. As the Board is aware, a MOU has been drafted and submitted for Gila River's review. Dale Shaw has made recent contact with a member of their public safety and is waiting to hear back. Any response from them will be communicated to the Board, as it is available.
- MPS Status
  - i. Mesa is working on establishing a communications link between the City of Mesa and Mesa Public Schools to be used in the event of a school emergency. This would allow Mesa PD and Fire to patch in with MPS Security and Administration to provide direct lines of communication, rather than rely on the traditional phone calls through dispatch. The two jurisdictions recently had a meeting to discuss protocol. An IGA is very close to being completed with MPS. This is just an informational update to the TRWC partners in the case that they would like to do something similar within their jurisdictions.
- Stimulus Funding
  - i. Mesa has inquired on several items related to stimulus funding, but to date has not yielded any funding. Alex Deshuk mentioned that COM Councilmember, Dennis Kavanaugh is going to Washington next week to lobby on the City's behalf for some relief on the requirements for funding.

## **Meeting Summary and Next Meeting Preview**

Topic Leader: Executive Director

- Chairman Cross summarized each of the agenda topics.
- The next Board of Director's meeting will be December 7 in Gilbert, same room and same time.
- Agenda Topics
  - Update on budget
  - Update on status of Rural Metro

## **Adjournment**

- Chairman Cross adjourned the meeting.

	<b>TRWC Policies and Procedures</b>	
<b>Owner:</b> <a href="#">See Below</a>	<b>Created:</b> 2009	<b>Applicability:</b> <a href="#">See Below</a>
<b>Category:</b> <b>Operations &amp; Maintenance</b>	<b>Revised:</b> 2009	
<b>Page:</b> 1 of 2	<b>Last Review:</b> 2009	

## 1.0 Purpose

- 1.1. The purpose of this policy is to define permissible communications and legitimate uses of the TOPAZ (Trunked **OP**en **Ar**iZona) Regional Wireless Cooperative (TRWC) network.

## 2.0 Owner

- 2.1. Administrative Manager

## 3.0 Applies To

- 3.1. Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the network.

## 4.0 Background

- 4.1. TRWC is a radio communications network that supports both public safety and public service operations and operates using frequencies licensed for such purposes by the Federal Communications Commission. Proper use of the TRWC network is required to ensure the system is available to support the intended purpose.

## 5.0 Policy Statement

- 5.1. The TRWC network is authorized by the Federal Communications Commission to use frequencies allocated for public safety and public service operations. As such, use of the TRWC network shall adhere to the restrictions related to permissible use of the frequencies.

## 6.0 Supporting Rules

- 6.1. Communications must be directly related and necessary to the support of public safety and public services operations.
- 6.2. Communications involving the imminent safety of life or property have the highest priority.

## 7.0 Responsibilities

- 7.1. Area Managers and Members are responsible for ensuring that appropriate training plans incorporate information on proper use of the TRWC network.

7.2. Area Managers and Members are responsible for appropriate and authorized use of talkgroups.

7.3. Interoperable talkgroups or shared talkgroups are only used for the designated purpose and only when authorized in accordance with the TRWC Governance Agreement, section 6.4.1.

## **8.0 Conditions for Exemption or Waiver**

8.1. None.

## **9.0 Applicable Procedures**

9.1. Governance Agreement

9.2. Talkgroup Plan Approval Policy

9.3. Network Security (category) policies

		<b>Maintenance &amp; Support Policy</b>	
Owner: <a href="#">See Below</a>	Created: 2009	Applicability: <a href="#">See Below</a>	
Category: Operations & Maintenance	Revised: 2009		
Page: 1 of 6	Last Review: 2009		

## 1.0 Purpose

- 1.1. The purpose of this policy is to establish the framework:
  - 1.1.1. Necessary to identify, resolve, and report anomalies that occur within TRWC in such a manner as to minimize the operational impact to participating agencies and their subscribers.
  - 1.1.2. Within which all maintenance activities pertaining to TRWC sites and facilities and TRWC infrastructure devices will be tracked and reported, including notification to Area Managers and Members of scheduled and unscheduled service affecting activities.

## 2.0 Owner

- 2.1. Administrative Manager

## 3.0 Applies To

- 3.1. Area Managers, Members, Associates, Interoperability Participants and Conditional Participants.
- 3.2. All personnel performing operations and planned or unplanned maintenance of the TRWC network infrastructure.

## 4.0 Background

- 4.1. The TRWC infrastructure is a critical enabling technology that supports public safety and public service operations with differing operational requirements. In anticipation of operational anomalies occurring within the network, and realizing that these anomalies must be triaged as expeditiously as possible, it is necessary to have policies in place that ensure network anomalies can be identified, reported, and resolved in a manner that minimizes the impact to Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the network.
- 4.2. The operational stability of TRWC may be affected when the configuration of the TRWC network is altered. Proper notification of scheduled and unscheduled service affecting maintenance activities will allow Members and Area Managers time to make necessary preparations. Conversely, unauthorized disruptions in TRWC operations caused by the lack of notification will create safety issues that must be addressed by the Administrative Manager.

## 5.0 Policy Statement

- 5.1. The Administrative Manager will establish and maintain the necessary processes and procedures relative to internal activities and third party support providers to ensure that operational and technical anomalies relative to TRWC are identified, triaged, and reported in such a fashion as to minimize the operational impact.
- 5.2. Members and Area Managers will be notified of any scheduled and unscheduled service affecting maintenance activities that have potential impact to the operational capabilities of the network.
- 5.3. All planned and unplanned maintenance activities will be tracked and reported.
- 5.4. A repository for tracking and reporting maintenance management data will be maintained by the administrative manager.

## **6.0 Supporting Rules**

- 6.1. At least twenty-four (24) hours advance notice will be given to Members and Area Managers prior to service affecting maintenance activities.
- 6.2. Service affecting maintenance activities not preceded by twenty-four (24) hours notice will be considered unscheduled maintenance.
- 6.3. Notification of unscheduled service affecting maintenance will be made to the Members and Area Managers as soon as practical.
- 6.4. Acceptable forms of notification would include phone, pager, e-mail, facsimile, or any other method as agreed to by the Administrative Manager, Area Managers, and Members.
- 6.5. At a minimum, the information contained in a notification will consist of:
  - 6.5.1. A description of the planned maintenance activity.
  - 6.5.2. The affected location(s) of the maintenance activity
  - 6.5.3. Anticipated operational impact.
  - 6.5.4. The scheduled start and stop time of the maintenance activity.
  - 6.5.5. The name of department or organization responsible for performing the activity.
- 6.6. Contact information for Members, Area Managers, and their designated alternates to be used for notification purposes will be kept in a central location and accessible from the Administrative Manager's wide area network.
- 6.7. No service affecting maintenance activities will be conducted during agency planned special operations.
- 6.8. All maintenance activities will be tracked in a database in accordance with procedures developed by the Administrative Manager.
- 6.9. All components of TRWC managed by the Administrative Manager shall be entered into a database and tracked.
- 6.10. Database Backups
  - 6.10.1. A multiple tape cycle backup method will be utilized for all database backups. The current backup tapes will be stored onsite at the server location. The backup prior to the current backup will be stored offsite at a secure location.
  - 6.10.2. Manual backups will be performed when the databases have undergone significant changes.
- 6.11. Configurations files and event logs will be backed up as determined by the Administrative Manager.

## 7.0 Responsibilities

- 7.1. The management of the TRWC infrastructure is the responsibility of the Administrative Manager.
- 7.2. The Administrative Manager will establish on-call after-hour support for anomaly resolution.
- 7.3. The Administrative Manager will ensure that TRWC reporting activities for anomalies will be conducted seven (7) days a week and twenty-four (24) hours a day.
- 7.4. The Administrative Manager will:
  - 7.4.1. Establish and maintain processes and procedures for operations and maintenance of the TRWC infrastructure.
  - 7.4.2. Identify and resolve network anomalies. Field service personnel will be dispatched when problems cannot be resolved remotely.
  - 7.4.3. Log problems and track them to closure.
  - 7.4.4. Analyze all logged problems to ensure network performance standards are maintained.
  - 7.4.5. Ensure that network log files are regularly reviewed and that cases are opened to resolve anomalies as necessary.
  - 7.4.6. Provide system performance reports.
  - 7.4.7. Maintain access to field replaceable units (FRUs) sufficient to mitigate equipment failures in a timeframe agreeable to TRWC Members.
  - 7.4.8. Maintain current software licensing on all TRWC infrastructure components.
  - 7.4.9. Maintain technical support necessary to operate, troubleshoot, and optimize the TRWC infrastructure.
  - 7.4.10. Incident types, response times, and appropriate actions are defined by severity level in accordance with procedures established by the Administrative Manager.
  - 7.4.11. Ensure that all operations and maintenance personnel, and third party support providers, are aware of this Maintenance & Support Policy; are trained in the appropriate processes, procedures, and response times; and have access to the necessary contact information to invoke various levels of support activities.
  - 7.4.12. Perform scheduled maintenance on the TRWC infrastructure in a manner that is consistent with industry best practices and manufacturer recommendations.
  - 7.4.13. Operate the TRWC network in accordance with the Network Security category policies.
  - 7.4.14. Responsible for notifying the Members and Area Managers of scheduled and unscheduled service affecting maintenance activities.
- 7.5. Mesa PD is the point of contact for key management and encryption. Requests for key management and encryption support are to be submitted to Mesa PD during normal business hours if possible. After hours, the point of contact for emergency support of key management and encryption is Mesa PD dispatch.
- 7.6. Area Managers and Members are responsible for providing their own dispatch console maintenance.
  - 7.6.1. Area Managers and Members are responsible for notifying the

Administrative Manager of maintenance activities on their consoles.

- 7.7. Area Managers and Members are responsible for communicating scheduled and unscheduled TRWC maintenance activities to their respective agencies and, if necessary, their respective dispatch centers.
- 7.8. Members and Area Managers are responsible for notifying Administrative Manager of the scheduling of planned special operations by their participating agencies.

## **8.0 Conditions for Exemption or Waiver**

- 8.1. Routine maintenance activities will be exempt from the notification process.

## **9.0 Applicable Procedures and Reference Document**

- 9.1. Change Control Policy

		<b>Change Control Policy</b>	
Owner: <a href="#">See Below</a>	Created: 2009	Applicability: <a href="#">See Below</a>	
Category: Configuration Management	Revised: 2009		
Page: 1 of 4	Last Review: 2009		

## 1.0 Purpose

- 1.1. The purpose of this policy is to ensure the proper change control processes and procedures are in effect to prevent unauthorized or harmful changes to the TRWC network infrastructure.
- 1.2. Changes will only be made to infrastructure configurations by following the procedures and approach described in this policy.

## 2.0 Owner

- 2.1. Administrative Manager

## 3.0 Applies to

- 3.1. All personnel attempting to make configuration changes to the production TRWC network infrastructure.
- 3.2. All TRWC network infrastructure components.

## 4.0 Background

- 4.1. Each component of the TRWC network infrastructure has a desired configuration that controls the operational capabilities of TRWC. Changes to the infrastructure configurations will be required from time to time. Because changes to infrastructure configurations have direct and immediate impact on the operational capabilities of the network, it is imperative that a policy exists to address how the configuration changes are requested, tested, approved, implemented and documented.

## 5.0 Policy Statements

- 5.1. Administrative control processes will be in effect at all times to ensure that all modifications to TRWC network infrastructure configurations are properly requested, analyzed, tested, approved, documented and implemented.
- 5.2. No service affecting modifications will be made to any TRWC infrastructure configurations without the review and approval of the Administrative Manager and in accordance with the "Maintenance & Support Policy."

### **Supporting Rules**

- 5.3. The Administrative Manager will coordinate all TRWC network infrastructure configuration changes.
- 5.4. All requests for network infrastructure configuration changes will be evaluated by the Administrative Manager for potential operational impact to subscriber agencies.
- 5.5. All network infrastructure parameter change requests will be reviewed by committees established by the Executive Director.
- 5.6. Each service affecting change to an infrastructure configuration will be thoroughly tested by the Administrative Manager.
- 5.7. Documentation shall be kept to provide an audit trail of the changes made to the network infrastructure configurations and to ensure that only the intended changes were made. Where applicable, output from configuration management software, electronic or hardcopy, shall be reviewed for accuracy and retained as part of the documentation package.

### **6.0 Responsibilities**

- 6.1. The Administrative Manager will be responsible for providing the committees established by the Executive Director with an overview of all network infrastructure parameter changes that includes a description of the change, benefits of implementation, a risk assessment, proposed implementation schedule, options and alternatives relative to the change, and a recommended course of action.
- 6.2. The committees established by the Executive Director will be responsible for reviewing proposed changes to the TRWC network infrastructure parameter(s), assessing the impact of the change request, and providing feedback (recommendation) to Administrative Manager relative to the change request.
- 6.3. The Administrative Manager will be responsible for ensuring that all affected parties are aware of the approved configuration change request and participate in the testing process as appropriate.
- 6.4. The Administrative Manager will be responsible for collecting and retaining all documentation relative to the infrastructure change.

### **7.0 Conditions for Exemption or Waiver**

- 7.1. Routine activities that result in changes to TRWC network infrastructure components such as adding subscribers to the UCS or other routine activities as determined by the Administrative Manager will be exempt from this policy.
- 7.2. During catastrophic events or emergency situations, immediate changes to the TRWC network infrastructure are authorized based on the judgment of the Administrative Manager, in consideration of all TRWC users, with

public safety considerations having the highest priority. The Administrative Manager will immediately notify the Executive Director, Members, and Area Managers, as time allows.

**8.0 Applicable Procedures**

8.1. Recommended form for Requests for Changes (following page of this policy)

8.2. Maintenance & Support Policy

## Requests for Changes will take the following form:

<b>REQUESTING AGENCY</b>	
<b>NAME OF REQUESTOR</b>	
<b>NEED BY DATE</b>	
<b>DESCRIPTION OF CHANGE</b>	
<b>PURPOSE OF CHANGE</b>	
<b>WORKGROUPS IMPACTED</b>	
<b>IMPACT EXPECTATION</b>	
<b>IMPLEMENTATION PLAN DEVELOPMENT (Task Definitions, Schedule, Responsibility, Recovery Strategy)</b>	
<b>ADMINISTRATIVE MANAGER RECOMMENDATION (section 6.1)</b>	
<b>FEEDBACK (RECOMMENDATION) FROM THE COMMITTEES ESTABLISHED BY THE EXECUTIVE DIRECTOR (section 6.2)</b>	
<b>ADDITIONAL COMMENTS</b>	

	<b>Talkgroup Plan Approval Policy</b>	
Owner: <a href="#">See Below</a>	Created: <b>2009</b>	Applicability: <a href="#">See Below</a>
Category: <b>Configuration Management</b>	Revised: <b>2009</b>	
Page: <b>1 of 2</b>	Last Review: <b>2009</b>	

### 1.0 Purpose

- 1.1. The purpose of this policy is to establish a process for talkgroup plan approval.

### 2.0 Owner

- 2.1 Administrative Manager

### 3.0 Applies To

- 3.1 Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the TOPAZ (Trunked **OP**en **Ar**iZona) Regional Wireless Cooperative (TRWC) network.

### 4.0 Background

- 4.1 A talkgroup is a defined organizational grouping of radio users that need to communicate together. When two or more radio users select the same talkgroup on their radios, all radio users with that talkgroup selection hear the transmitted audio. A talkgroup plan is the summary of all defined radio talkgroups. This plan is then used to develop the radio template which is the programming data for the individual radios.

### 5.0 Policy Statement

- 5.1 As talkgroup plans are designed to support public safety and public service operations for the Members, and have a direct impact to TRWC system performance, the Administrative Manager will review and approve all talkgroup plans and proposed changes.

### 6.0 Supporting Rules

- 6.1 Each Area Manager's and Member's agencies are responsible for development of their talkgroup plans.
  
- 6.2 As the number of talkgroups has a direct impact to system performance, all proposed talkgroup plans should consider possible impacts to system loading and performance.

- 6.3 Each agency using TRWC will develop a preliminary talkgroup plan that considers internal business operations and any requirements for communications with other TRWC entities.
- 6.4 Upon completion of the preliminary talkgroup plan, the agency shall submit the preliminary plan to the Administrative Manager for technical and operational analysis.
- 6.5 The Administrative Manager will complete a technical review and provide the committees established by the Executive Director with an analysis on system performance related to the proposed talkgroup plan.
- 6.6 The committees established by the Executive Director will consider the preliminary talkgroup plans and all supporting information and recommend approval of the request or make a recommendation for changes to the requesting agency.

## **7.0 Responsibilities**

- 7.1 The Administrative Manager is responsible for maintaining a database of all approved talkgroup plans.

## **8.0 Conditions for Exemption or Waiver**

- 8.1 None

## **9.0 Applicable Procedures**

- 9.1 Governance Agreement, section 6.4.1

	<b>System Key Control Policy</b>	
<b>Owner:</b> <a href="#">See Below</a>	<b>Created:</b> 2009	<b>Applicability:</b> <a href="#">See Below</a>
<b>Category:</b> <b>Network Security</b>	<b>Revised:</b> 2009	
<b>Page:</b> 1 of 2	<b>Last Review:</b> 2009	

### 1.0 Purpose

- 1.1. The purpose of this policy is to establish the controls for the TRWC System Key used for subscriber unit programming.

### 2.0 Owner

- 2.1. Administrative Manager

### 3.0 Applies To

- 3.1. Anyone that has access to the TRWC subscriber programming software.

### 4.0 Background

- 4.1. TRWC is a radio communications network that provides services and features to radio users through the programming software of the subscriber radios. Programming of the subscriber radios is controlled by an electronic "System Key." As this programming application directly affects the TRWC public safety and public service department operations it is important that the System Key is protected from potential security related risks that can cause disruptions or anomalies to subscriber operations.
- 4.2. The System Key must be programmed into any subscriber unit that operates directly on TRWC. These subscriber units include all Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants, and could also include radio units from other entities that are given access rights to use TRWC.
- 4.3. TRWC public safety departments have operational requirements and mutual aid agreements that require they interoperate with non-TRWC entities. Direct interoperability (automatic unit to unit) is supported by programming non-TRWC subscriber equipment with the TRWC System Key. Please refer to section 4.1.5 of the Governance Agreement.
- 4.4. The risk of inaccurate programming substantially increases when multiple entities are allowed access to and use the System Key to program subscriber units. This risk translates into an increase in subscriber radio operational anomalies and the associated administrative/maintenance activities. There is also an increased risk of possible unauthorized transmissions, interference or monitoring of public safety radio communications channels.

## **5.0 Policy Statement**

- 5.1. Anyone that has access to the TRWC subscriber programming equipment shall at all times employ appropriate operational and network security practices, as adopted by the Administrative Manager, to protect TRWC users from programming errors that could potentially cause disruptions or failures in service.
- 5.2. The Administrative Manager will control the TRWC System Key. The TRWC System Key will not be released to Area Managers, Members, Associates, Interoperability Participants, Conditional Participants, or their Contractors.

## **6.0 Supporting Rules**

- 6.1. The Administrative Manager will provide all routine and emergency TRWC radio programming services for the Area Manager, Members, Associates, Interoperability Participants, and Conditional Participants as defined in the TRWC Governance Agreement.
- 6.2. Requests for programming of the TRWC System Key into non-TRWC radios shall be made by the appropriate representative of the requesting agency to the Executive Director.
- 6.3. The Administrative Manager will provide, upon approval by the Executive Director, programming services for authorized non-TRWC radios for interoperable service as defined in section 4.1.5 of the TRWC Governance Agreement.
- 6.4. Any breaches in TRWC System Key use shall immediately be reported to the Administrative Manager and Executive Director who shall take immediate steps to minimize the danger to the operational capabilities of TRWC.

## **7.0 Responsibilities**

- 7.1. The Administrative Manager is responsible for the development of internal controls for protection of the TRWC System Key.
- 7.2. The Administrative Manager or designee is responsible for monitoring issues related to use of the System Key, and to report actions involving misuse of the System Key to the Administrative Manager and Executive Director for resolution.

## **8.0 for Exemption or Waiver**

- 8.1. None

## **9.0 Applicable Procedures**

- 9.1. TRWC Governance Agreement

	<b>Password Administration Policy</b>	
<b>Owner:</b> <a href="#">See Below</a>	<b>Created:</b> 2009	<b>Applicability:</b> <a href="#">See Below</a>
<b>Category:</b> Network Security	<b>Revised:</b> 2009	
<b>Page:</b> 1 of 3	<b>Last Review:</b> 2009	

## 1.0 Purpose

- 1.1. The purpose of this policy is to establish a standard for the creation of passwords for access to the TRWC Network in order to prevent unauthorized read or write access.

## 2.0 Owner

- 2.1. Administrative Manager

## 3.0 Applies To

- 3.1. All personnel who have or are responsible for an account, or any form of access that supports or requires a password.

## 4.0 Background

- 4.1. There are multiple software applications, protected by password access only, available in the TRWC system. Access privileges provide critical configuration and security information that make it imperative to control the viewing, modification, and potential dissemination of this information. Unauthorized access, whether malicious or unintentional, must not be permitted.

## 5.0 Policy Statement

- 5.1. The Administrative Manager will establish and maintain the necessary processes and procedures to ensure that passwords to include the read, write, and executable functions of the TRWC system applications, components and interfaces are restricted to authorized users.

## 6.0 Supporting Rules

- 6.1. Users will not loan, share, divulge, or otherwise make accessible their password(s) to other individuals. All passwords are to be treated as sensitive and confidential information.
- 6.2. Passwords must not be inserted into email messages or other forms of electronic communication.
- 6.3. TRWC passwords should contain both upper and lower case letters when applicable.
- 6.4. TRWC passwords should have numbers (0-9) and letters.
- 6.5. TRWC passwords must be at least eight characters in length.

- 6.6. TRWC passwords must not be based on personal information, names of family, etc.
- 6.7. Derivatives of user-IDs and common character sequences such as "123456" must not be employed.
- 6.8. Personal details such as license plate, social security number, or birthday must not be used. Passwords created by using a proper name, geographic location, common acronym, or slang, must be made unique by inserting special characters or through combinations of characters or words that would be difficult to duplicate.
- 6.9. TRWC users must not create passwords that are identical or substantially similar to passwords they previously employed.
- 6.10. TRWC passwords should never be written down or stored on-line.
- 6.11. TRWC users must not use the same password for TRWC accounts as for other non-TRWC access.
- 6.12. TRWC users must not use the "Remember Password" feature of any TRWC applications.
- 6.13. The interval for changing passwords will be set at a maximum of 35 days.
- 6.14. New passwords issued must be valid only for the authorized user's first on-line session. Upon initial access, the user must choose another password before any other work is done.
- 6.15. If an account or password is suspected of having been compromised it must be reported to the Administrative Manager immediately.

## **7.0 Responsibilities**

- 7.1. The Administrative Manager will publish and provide a recommended form for Electronic Access Requests to all requesting agencies. All access requests will be subsequently reviewed and a response provided to the requestor in a timely manner.
- 7.2. The Administrative Manager will conduct a password audit and provide the Executive Director, on a regular basis, with user profile reports showing personnel access to key infrastructure components, user databases, component operating systems and system interfaces.
- 7.3. The Administrative Manager will ensure that all TRWC personnel are aware of the Password Administration Policies.
- 7.4. The Administrative Manager will monitor, through manual audits of log files or automated software, any access attempts deemed of a suspicious or malicious nature. Suspicious or malicious access attempts will be reported to the Executive Director.
- 7.5. The Administrative Manager will maintain all electronic access request records.
- 7.6. The Administrative Manager will maintain a centralized user access control list to determine, audit and report who is authorized to access the network.

7.7. Personnel and contractors involved in the support of TRWC will acknowledge the receipt, comprehension and adherence of the TRWC Password Administration Policies by signature which will be returned to the Administrative Manager.

**8.0 Conditions for Exemption or Waiver**

8.1. In the event an emergency, the Administrative Manager has the capability to provide immediate access to personnel on a case-by-case basis.

**9.0 Applicable Procedures and Reference Documents**

9.1. Recommended form for Electronic Access Requests

	<b>Access to Administrative Functionality Policy</b>	
<b>Owner:</b> <a href="#">See Below</a>	<b>Created:</b> 2009	<b>Applicability:</b> <a href="#">See Below</a>
<b>Category:</b> Network Security	<b>Revised:</b> 2009	
<b>Page:</b> 1 of 2	<b>Last Review:</b> 2009	

## 1.0 Purpose

- 1.1. The purpose of this policy is to limit electronic access to the TRWC administrative functions to prevent unauthorized administrative changes and provide a method for user accountability.

## 2.0 Owner

- 2.1. Administrative Manager

## 3.0 Applies to

- 3.1. All personnel attempting to make modifications to TRWC user databases, infrastructure programming, and component operating systems.

## 4.0 Background

- 4.1. There are multiple software tools available in the TRWC network that provides useful administrative functionality to network management and operations and maintenance personnel. The administrative privileges also provide critical configuration and security information that make it imperative to control the read and write functions of files and potential dissemination of this information.

## 5.0 Policy Statement

- 5.1. Administrative access to include the read, write and executable functions of the TRWC system administrative tools is restricted to users authorized by the Administrative Manager.

## 6.0 Supporting Rules

- 6.1. Personnel with electronic access to the administrative functions of TRWC are required to have a current, signed recommended form for Electronic Access Request on file with the Administrative Manager. These documents may be subject to renewal at regular intervals.
- 6.2. The Administrative Manager will review all request for electronic access using appropriate justification and verification processes.
- 6.3. Administrative users will be granted levels of access (read, write, execute) to programs based on the minimum necessary to perform their job.
- 6.4. If any person discovers they have inadvertently been allowed access to a programming function not required to perform their job or are uncertain

about their privilege level, they will report it to the Administrative Manager immediately.

## **7.0 Responsibilities**

- 7.1. The Administrative Manager is responsible for ensuring the approved administrative access to the system is currently required to perform personnel work duties and the type of access required matches the current privilege level.

## **8.0 Conditions for Exemption or Waiver**

- 8.1. None

## **9.0 Applicable Procedures**

- 9.1. Recommended form for Electronic Access Requests
- 9.2. Remote Access Policy
- 9.3. Password Administration Policy

	<b>Remote Access Policy</b>	
<b>Owner:</b> <a href="#">See Below</a>	<b>Created:</b> 2009	<b>Applicability:</b> <a href="#">See Below</a>
<b>Category:</b> <b>Network Security</b>	<b>Revised:</b> 2009	
<b>Page:</b> 1 of 3	<b>Last Review:</b> 2009	

## 1.0 Purpose

- 1.1. The purpose of this policy is to minimize the risks associated with provisions for remote access to the TRWC network.

## 2.0 Owner

- 2.1. Administrative Manager

## 3.0 Applies To

- 3.1. Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the network, and all contractors.
  
- 3.2. This policy covers all TRWC system software and infrastructure components that are accessible via remote access including, but not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, terminal server connectivity, or remote control software.

## 4.0 Background

- 4.1. The TRWC system is comprised of a multitude of components that inherently have the capability for a user to communicate with the target component from a remote location via a pre-determined login/password routine. In some instances this capability may allow off-site personnel to perform diagnostics and resolve system trouble without traveling to the physical location.

## 5.0 Policy Statement

- 5.1. Remote access to TRWC is prohibited unless expressly permitted by the Administrative Manager.

## 6.0 Supporting Rules

- 6.1. All Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the network and contract vendors are required to submit in writing to the Administrative Manager, in advance, their requests for remote access to TRWC using the recommended form for Electronic Access Requests (or equivalent) including the general functions and expected duration of the tasks to be performed via the remote connection.

- 6.2. All remote access request responses from the Administrative Manager will be returned to the requesting organization with an explanation for denial or approval.
- 6.3. Remote connections are not permitted to retrieve files from inside TRWC.
- 6.4. Any computer permitted remote access to the TRWC network requires certification to the Administrative Manager that the computer has the latest virus definitions, operating system patches, and is in compliance with all security configuration requirements.
- 6.5. Any computer used to remotely access the TRWC network and physically connects to other public or private networks (i.e. - VPN) shall be capable of using encryption.
- 6.6. Individuals or their agency representative will promptly notify the Administrative Manager whenever any user who has been granted remote access no longer requires access to the TRWC network or TRWC related equipment.
- 6.7. Any computer with the ability to access TRWC and other non-TRWC networks must be configured with a personal firewall, virus protection software, or equivalent to protect against viral propagation between networks.
- 6.8. Any individual or company granted TRWC remote access will not share, publish, or divulge by any means, connection information, including but not limited to, modem numbers, ISDN numbers, IP addresses, access codes, passwords, logins, and secure tokens.

## **7.0 Responsibilities**

- 7.1. The Administrative Manager will establish and maintain the necessary processes and procedures to prohibit, unless expressly permitted, remote access to TRWC infrastructure components and system software to include, but not be limited to, network transport, RF infrastructure, site equipment, the Private Radio Network Management Suite (PRNM) and the Core Security Management Suite (CSMS).
- 7.2. The Administrative Manager will ensure that a centralized user access control list will be maintained to determine, audit and report who is authorized to remotely access TRWC.
- 7.3. The Administrative Manager will conduct a remote access audit to generate and maintain user profile reports showing personnel, including vendors, with remote access to key infrastructure components, system software, user databases, and component operating systems.
- 7.4. The Administrative Manager will notify the Executive Director of any remote access attempts deemed of a suspicious or malicious nature.

- 7.5. The Administrative Manager will ensure that any changes to firewall configurations and/or access control lists will be reviewed and approved.
- 7.6. The Administrative Manager will ensure that all Area Managers, Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the network, and contract support providers, are aware of the Remote Access Network Policies, and have access to the necessary contact information to request remote access for their personnel.

**8.0 Conditions for Exemption or Waiver**

- 8.1. None

**9.0 Applicable Procedures and Reference Documents**

- 9.1. Recommended form for Electronic Access Requests



**Recommended Form for  
Electronic Access Request**

Owner: <a href="#">See Below</a>	Created: 2009	Applicability: <a href="#">See Below</a>
Category: Network Security	Revised: 2009	
Page: 1 of 1	Last Review: 2009	

**To be completed by Electronic Access Requester**

Name \_\_\_\_\_

Agency/  
Department \_\_\_\_\_

Date \_\_\_\_\_

Functionality Requested \_\_\_\_\_

Reason for Request \_\_\_\_\_

Duration Required \_\_\_\_\_

Request for Access and  
Acknowledgement of TRWC  
Password Administration Policy \_\_\_\_\_

**To be completed by Administrative Manager**

Access Granted Date: \_\_\_\_\_



# Rural/Metro Fire Department

Maricopa / Pinal County Operations ♦ 708 West Baseline Road ♦ Mesa, AZ 85210  
Office 480-655-7404 Fax 480-655-7403

Dale Shaw  
Executive Director, TOPAZ Regional Wireless Cooperative  
PO Box 1466  
Mesa, AZ 85201-6613

Dear Mr. Shaw,

Firefighter and public safety is paramount to our collective mission as fire professionals. Time and time again, lack of communications on a fire ground has lead to firefighter injuries, or worse, firefighter deaths. A seamless interoperability communication system will significantly enhance our duty to further protect our firefighters.

The Rural/Metro Fire Department is seeking acceptance into the TOPAZ Regional Wireless Cooperative (TRWC) as an Interoperability Participant under Section 4.1.5. As part of this cooperative, we will purchase the equipment required to provide a seamless chain of communication throughout all fire ground activities with other TRWC participants.

Rural/Metro Fire will provide up to 40 radios over a two year span to meet this goal. We will also provide the necessary training and maintenance agreements to accomplish this.

Thank you in advance for your consideration. We look forward to meeting with the TRWC Board of Directors to present our request in person.

Yours in Life Safety,

Dan Caudle  
Fire Chief, Rural/Metro



# HIGH PERFORMANCE DATA SYSTEM (HPD)

# EXISTING UHF DATA SYSTEM

**Obsolete Technology**

~~~~~

**Relatively Slow Speed – 9.6 kbps**

~~~~~

**No Longer Supported By Manufacturer  
(Replacement Parts Difficult to Find)**

~~~~~

**FCC Mandated Migration to Narrowband Frequencies  
(January 2013 Deadline)**

# **HIGH PERFORMANCE DATA SYSTEM (HPD)**

**Private Network for Mission Critical  
Public Safety Applications**

~~~~~

**Assured Communications**

~~~~~

**Not Dependant Upon Commercial Wireless Services  
That Are Likely to be Overloaded During a Major Event**

~~~~~

**Motorola HPD Technology Data Rates up to 96kbps**

# **HIGH PERFORMANCE DATA SYSTEM (HPD)**

**Reliable 700 MHz Radio Infrastructure**

~~~~~

**Industry Standard IP Based Routing Protocol**

~~~~~

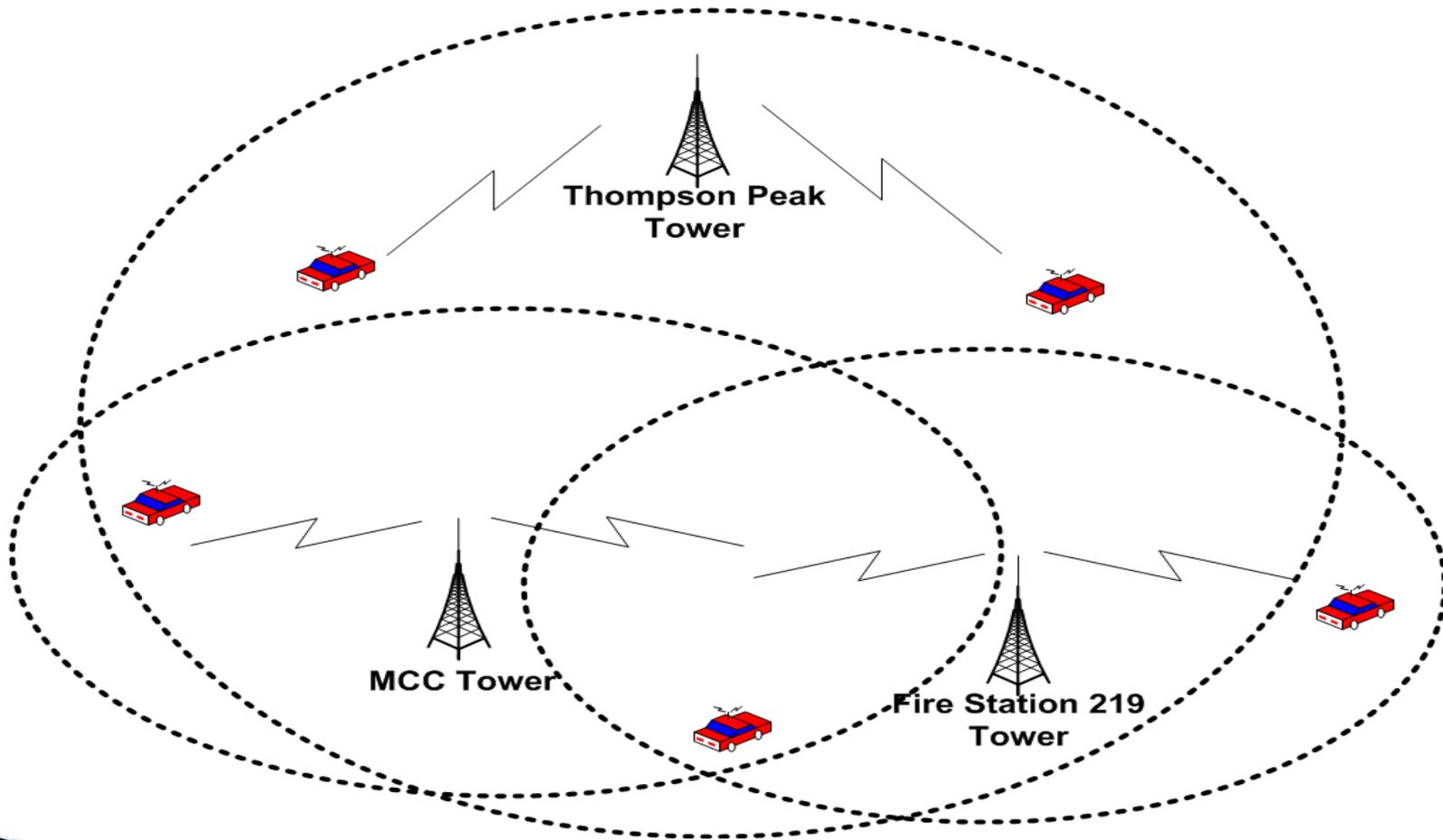
**Fast, Reliable, Secure Delivery of Messages**

# Radio-IP Hybrid Solution

**RadiolP Middleware Integrates the Public Safety HPD Radio System and Commercial or Private Broadband Services (WI-FI, WIMAX, EV-DO, Mesh, etc.)**

**Non-Mission Critical Applications That Require Higher Bandwidth Can Be Automatically Routed to Commercial or Private Broadband Wireless Services Where Available**

# HIGH PERFORMANCE DATA SYSTEM (HPD)



# HPD 700 MHz RADIO MODEM



# HPD Infrastructure

- ▶ Three Single Channel Transmitter/ Receiver Sites (Thompson Peak, Fire Station 219, MCC)
- ▶ Integrated into Existing City Microwave Network

## Infrastructure Costs

▶ Motorola GTR8000 – 700 MHz Stations	\$360,767
▶ Systems Integration	\$366,700
▶ Radio IP Middleware Infrastructure	\$79,773
▶ Server for Radio IP (Estimated)	<u>\$25,000</u>
Total	\$832,240

# **Transition Timeline**

**Submit Application to FCC for Radio Frequencies  
(3 to 4 Months)**

**Infrastructure Installation and Testing  
(6 to 8 Months)**

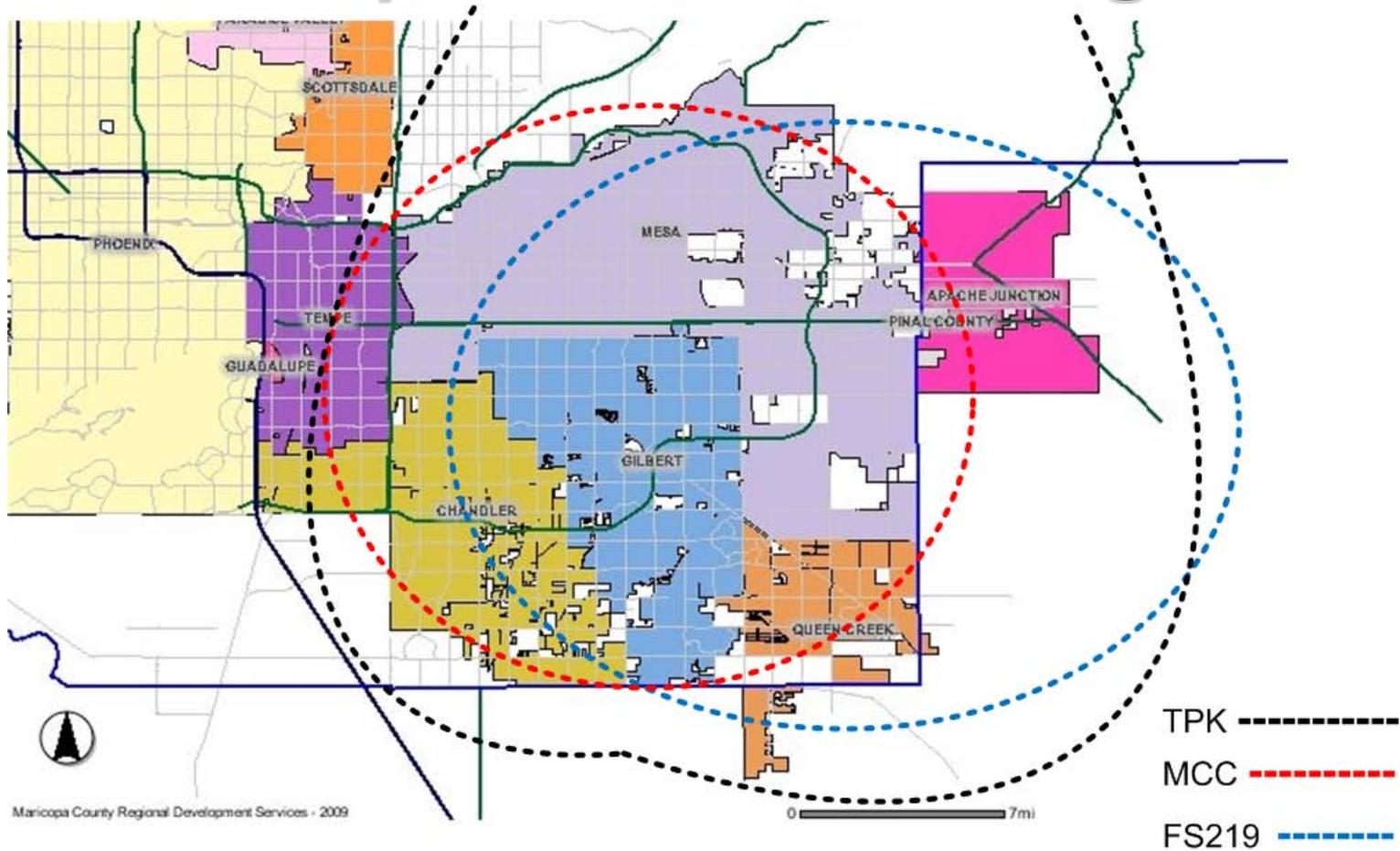
**UHF System Continues Operation During Transition  
to HPD System**

**Installation of Mobile Units**

**Retired Units can be Used as Spares on Old System**

**Decommissioning of Old UHF System**

# 700 MHz HPD Data System Proposed RF Coverage



**TOPAZ FINANCIAL REVIEW  
PRESENTED TO BOARD OF DIRECTORS SEPTEMBER 14, 2009**

**RECAP OF FISCAL YEAR 2008/2009 [JANUARY 2009 THRU JUNE 2009]**

**OPERATIONS**

	COM	TOG	AJFD	CAJ	TQC	TOTAL
Budgeted Subscriber Units as of 12-17-2008	2,734	712	74	164	4	3,688
Actual Subscriber Units as of 7-1-2009	2,754	730	74	164	27	3,749
Difference	20	18	0	0	23	61
Percentage Increase	0.73%	2.53%	0.00%	0.00%	575.00%	1.65%

	COM	TOG	AJFD	CAJ	TQC	TOTAL	% of BUDGET	YTD VARIANCE	6 MONTH BUDGET	ANNUAL BUDGET
Budgeted Cost Per Radio For Initial 6 Months	\$502,230	\$130,794	\$13,596	\$30,126	\$732	\$677,478			\$677,478	\$1,354,956
						\$31				
Actual Cost Per Radio For Initial 6 Months	\$412,893	\$109,261	\$11,065	\$24,520	\$3,375	\$561,114	82.82%			
Difference	-\$89,337	-\$21,533	-\$2,531	-\$5,606	\$2,643	-\$116,364		-17.18%		
						\$25				

**RECAP OF FISCAL YEAR 2009/2010**

**OPERATIONS**

	COM	TOG	AJFD	CAJ	TQC	TOTAL
Budgeted Subscriber Units as of 3/10/2009	2,770	741	74	164	26	3,775

	COM	TOG	AJFD	CAJ	TQC	TOTAL	
Budgeted Cost Per Radio	\$89,735	\$24,005	\$2,397	\$5,313	\$842	\$122,292	\$1,467,506
						\$32	

**CAPITAL**

	COM	TOG	AJFD	CAJ	TQC	TOTAL
Costs To Reconfigure and White Tanks	\$944,735	\$252,725	\$25,238	\$55,934	\$8,868	\$1,287,500
[Billing in January, February, March 2010]	\$314,912	\$84,242	\$8,413	\$18,645	\$2,956	\$429,167

**POTENTIAL CHANGE IN CASH FLOW PROJECTIONS FOR CAPITAL COSTS**

1. Costs To Reconfigure \$721,000

<u>Contract Terms</u>	Expected Execution	Amount	BOD Consideration
25% due on contract execution	Jul-09	\$170,000	Cost incurred, bill partners now rather than January-March 2010
60% due on shipment of equipment	Dec-09		No Cash Flow Change
	December 2009 to		
5% due on installation of equipment	January 2010		No Cash Flow Change
5% due on system acceptance	Feb-10		No Cash Flow Change
5% due on final acceptance	March-April 2010		No Cash Flow Change

2. White Tanks \$566,500

<u>Contract Terms</u>	Expected Execution	Amount	BOD Consideration
70% due on delivery	Sep-09	\$210,000	Cost incurred, bill partners now rather than January-March 2010
20% due on completion of acceptance test	March-April 2010		No Cash Flow Change
10% due on final acceptance	March-April 2010		No Cash Flow Change

3. Impact On Cash Flow To Partners

	COM	TOG	AJFD	CAJ	TQC	TOTAL
Budgeted Cash Flow From Above	\$944,735	\$252,725	\$25,238	\$55,934	\$8,868	\$1,287,500
Bill 25% Due On Contract Execution Now - Reconfiguration	\$124,742	\$33,370	\$3,332	\$7,385	\$1,171	\$170,000
Bill 70 % Due On Contract Delivery September-October 2009 for White Tanks	\$154,093	\$41,221	\$4,117	\$9,123	\$1,446	\$210,000
Revised Cash Flow	\$665,901	\$178,134	\$17,789	\$39,425	\$6,251	\$907,500
[Billing in January, February, March 2010]	\$221,967	\$59,378	\$5,930	\$13,142	\$2,084	\$302,500

**TOPAZ BUDGET TO ACTUAL COMPARISON**  
**Reconfiguration and White Tanks Capital Projects**  
**Fiscal Year 2009 / 2010**

**1. Budgeted Subscriber Units (As of 3-10-2009)**

COM	TOG	AJFD	CAJ	TQC	TOTAL
<b>2,770</b>	<b>741</b>	<b>74</b>	<b>164</b>	<b>26</b>	<b>3,775</b>
73.38%	19.63%	1.96%	4.34%	0.69%	100.00%

**2. Budgeted Capital Costs**

COM	TOG	AJFD	CAJ	TQC	TOTAL
<b>\$944,735</b>	<b>\$252,725</b>	<b>\$25,238</b>	<b>\$55,934</b>	<b>\$8,868</b>	<b>\$1,287,500</b>
<b>\$529,052</b>	<b>\$141,526</b>	<b>\$14,134</b>	<b>\$31,323</b>	<b>\$4,966</b>	<b>\$721,000</b>
<b>\$415,683</b>	<b>\$111,199</b>	<b>\$11,105</b>	<b>\$24,611</b>	<b>\$3,902</b>	<b>\$566,500</b>

**a. Reconfiguration**

**b. White Tanks**

**3. Actual Costs Incurred**

**July and August Costs**

**a. Reconfiguration**

**b. White Tanks**

**c. Total Due For July and August**

COM	TOG	AJFD	CAJ	TQC	TOTAL
\$123,147	\$32,943	\$3,290	\$7,291	\$1,156	\$167,826
\$4,545	\$1,216	\$121	\$269	\$43	\$6,195
\$127,692	\$34,159	\$3,411	\$7,560	\$1,199	\$174,021

## HDP Subscriber Equipment Pricing

Department	# of Units	HPD Modem	Radio-IP Client	Total
City of Mesa Fire *	85	\$120,904.00	\$29,622.50	\$150,526.50
Mesa Police *	380	\$540,512.00	\$132,430.00	\$672,942.00
Apache Junction Fire	20	\$32,004.00	\$6,970.00	\$38,974.00
Gilbert Fire	41	\$65,608.20	\$14,288.50	\$79,896.70
Queen Creek Fire	7	\$11,201.40	\$2,439.50	\$13,640.90
Southwest Ambulance	44	\$70,408.80	\$15,334.00	\$85,742.80

Note: Above pricing is based on individual purchases by department based on quantities in service today. Additional discounts may be possible by group purchases (See below).

\* Mesa pricing is based on MFD & MFD placing order at same time.

	Pricing - Based on Quantity Ordered		
HPD Radio Modem	1-100	100-400	400 +
HPD Radio Modem -Price Per Unit	\$1,600.20	\$1,511.30	\$1,422.40
Radio-IP Client Software	\$348.50	n/a	n/a