

**SUBMITTAL TO THE BOARD OF SUPERVISORS  
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA**

341



**FROM:** Public Safety Enterprise Communication Steering Committee  
(PSEC)

**SUBMITTAL DATE:**  
October 4, 2012

**SUBJECT:** Approval of the PSEC Radio System Business Plan, Establishment of an Internal Service Fund, and amend Ordinance No. 440 pursuant to Resolution No. 440-8909.

**RECOMMENDED MOTION:** That the Board of Supervisors:

1. Adopt the attached PSEC business plan (Attachment A);
2. Amend Ordinance No. 440 pursuant to Resolution No. 440-8909 submitted herewith;
3. Approve and direct the Auditor Controller to establish an interest earning Internal Service Fund for PSEC;
4. Approve and direct the Auditor Controller to make the budget adjustment for the PSEC budget (Attachment C);
5. Approve and direct the Auditor Controller to coordinate with RCIT to transfer a 30-day working capital to the new ISF;
6. Approve amendments to Board Policy B-26 – Leasing of County-Owned Real Property For Wireless Service Facilities (Attachment B);
7. Approve and direct the Auditor Controller to coordinate with RCIT the transfer of PSEC capital assets to a general fund account;
8. Approve the creation of the PSEC Governance Board and delegate authority to establish by-laws and membership; and
9. Approve the PSEC rates as per Exhibit B of the PSEC Business Plan (Attachment A)

**FISCAL PROCEDURES APPROVED**  
 PAUL ANGULO, CPA, AUDITOR-CONTROLLER  
 BY *Paul Angulo*  
 TANYA SCHARRIS, CPA

Departmental Concurrence

Approved by Barbara A. Oliver,  
 Asst. County Executive Officer/  
 Human Resources Director

<i>Colleen Walker</i> Stan Sniff Sheriff-Coroner-PA	<i>John Hawkins</i> John Hawkins Chief, County Fire	<i>Wesley P. Colvin for Kevin K. Crawford 10/4/2012</i> Kevin K Crawford Chief Information Officer
---	---	--

Current F.Y. Total Cost:	\$9,217,426	In Current Year Budget:	No
Current F.Y. Net County Cost:	\$ 0	Budget Adjustment:	Yes
Annual Net County Cost:	\$ 0	For Fiscal Year:	FY 12/13

<b>SOURCE OF FUNDS:</b> Internal Service Fee Charges	<b>Positions To Be Deleted Per A-30</b>	<input type="checkbox"/>
	<b>Requires 4/5 Vote</b>	<input checked="" type="checkbox"/>

**C.E.O. RECOMMENDATION:** APPROVE.

*Christopher Hans*

County Executive Office Signature By Christopher Hans

**MINUTES OF THE BOARD OF SUPERVISORS**

On motion of Supervisor Ashley, seconded by Supervisor Tavaglione and duly carried by unanimous vote, IT WAS ORDERED that the above matter is approved as recommended, Resolution 440-8909 is adopted, and IT WAS FURTHER ORDERED THAT the voting makeup of the Governance Board come back to the Board for approval.

Ayes: Buster, Tavaglione, Stone, Benoit and Ashley  
 Nays: None  
 Absent: None  
 Date: October 16, 2012

Kecia Harper-Ihem  
 Clerk of the Board  
 By: *Kecia Harper-Ihem*  
 Deputy

Prev. Agn. Ref.: 09/12/05 3.44a  
 01/30/07 3.42b, 03/31/09 3.33  
 02/09/10 3.41

Agenda Number:

ATTACHMENTS FILED  
WITH THE CLERK OF THE BOARD

3.35 a

Dept Recomm.:  Policy  
 Per Exec. Ofc.:  Policy  
 Consent:

## **BOARD OF SUPERVISORS**

### **FORM 11: Approval of the PSEC Radio System Business Plan, Establishment of an Internal Service Fund, and amend Ordinance No. 440 pursuant to Resolution No. 440-8909**

PAGE 2

#### **BACKGROUND:**

In January 2007, the Board of Supervisors awarded Motorola, Inc. a contract to resolve the county's radio coverage challenges (Item 3.42b). The Board established an Executive Steering Committee to include key executive staff from the Sheriff's Department, Fire Department, Facilities Management (EDA), RCIT and the Executive Office to monitor the project's progress and make high-level decisions. In March 2009, the Board of Supervisors approved the PSEC Radio System Detail Design and authorized the PSEC Steering Committee to proceed with the implementation of the PSEC Project (Item 3.33).

County departments are scheduled to begin migrating onto the PSEC radio system in November 2012. In preparation for the cutover date, we are requesting establishment of a unique fund for the radio system separate from all other RCIT operating costs. The purpose of the separate fund is to provide transparency of all radio costs associated with the new radio system.

The annual cost for the new radio system is \$14.4 million and will be supported by the revenue collected from county departments and outside agencies. Existing subscribers (radio customers) will continue to pay the current radio system rates through December 2012. Effective January 1, 2013, radio customers will begin paying the new radio system fees in accordance with the attached rate sheet.

As a result of the new system, additional service offerings have been developed that are currently available for use. For these services, RCIT is requesting that the specific rates as identified on the rate sheet become effective now to fulfill immediate service needs. The new radio system budget and rates have been reviewed and approved by the PSEC Steering Committee.

The PSEC project team has developed a budget based on anticipated costs to support the new system. However, as this is a first-of-its-kind radio system, there may be unknown factors that will require budgetary adjustments.

#### **IMPLEMENTATION**

The success of a major project such as PSEC in Riverside County requires a process that includes post-implementation stakeholder oversight, strategic direction, collaboration and planning for long term efficient operation and interoperability. Interoperability will require the commitment of multiple disciplines from the public safety community and executive leadership in County government.

**Background:** (continued)

Following system implementation, the PSEC Steering Committee will transition to the Governance Board. The PSEC Governance Board will establish the appropriate foundational environment in which this collaboration and high-level operational oversight of the PSEC system will be maintained.

The responsibilities of the PSEC Governance Board will include, but not limited to, review of the PSEC annual operational budget (which will include prioritizing project requests and system upgrades, support staffing requirements and system rates) prior to submittal to the Board of Supervisors for approval; policies for regulation of system and its use, and approve additional system users.

The Governance Board will initially be comprised of the following, or designated alternate:

- Riverside County Board of Supervisor member – Voting Seat
- Riverside County Sheriff – Voting Seat
- Riverside County Fire Chief - Voting Seat
- County Executive Officer – Voting Seat
- Chief Information Officer – Voting Seat
- Future members, of which up to 4 will be selected to fill voting seats, may include:
  - Local Municipal Police Departments / Fire Agencies;
  - Other Municipal agencies;
  - State and Federal Agencies;
  - Educational Agencies or Institutions; and
  - Non-governmental Organizations.
- Other County of Riverside Agencies or Departments – Non-voting Seats

The PSEC Governance Board will define a process to determine public safety and public service entities participation in the PSEC Governance Board, including which agencies will hold voting seats.

The PSEC Governance Board will approve the allocation of budgetary costs associated with the system operations, user rates, and system maintenance costs, via the County Annual Budgetary process, prior to seeking Board of Supervisor approval. RCIT is responsible for both the day-to-day administration of the approved budget and operational support and maintenance of the PSEC system.

RESOLUTION NO. 440-8909

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

BE IT RESOLVED by the Board of Supervisors of the County of Riverside, State of California, in regular session assembled on October 16, 2012, that pursuant to Section 4(a)(ii) of Ordinance No. 440, the Chief Information Officer is authorized to make the following listed change(s), operative on the date of approval, as follows:

<u>Job Code</u>	<u>+/-</u>	<u>Department ID</u>	<u>Class Title</u>
76431	- 1	7400300000	Radio Communications Engineer I
76431	+ 1	7400151210	Radio Communications Engineer I
86127	+ 1	7400151210	IT Communications Technician I
86125	+ 1	7400151210	IT Supervising Communications Analyst
15826	+ 4	7400151210	Support Services Technician

BE FURTHER IT RESOLVED that pursuant to Section 4(a)(ii) of Ordinance No. 440, the Chief Information Officer is authorized to make the following listed change(s), with an operative date of January 1, 2013, as follows:

<u>Job Code</u>	<u>+/-</u>	<u>Department ID</u>	<u>Class Title</u>
74106	- 1	7400300000	Administrative Services Analyst II
74106	+ 1	7400600000	Administrative Services Analyst II
86124	- 4	7400300000	IT Communications Analyst III
86124	+ 1	7400151400	IT Communications Analyst III
86124	+ 3	7400600000	IT Communications Analyst III
86127	- 1	7400151210	IT Communications Technician I
86127	+ 1	7400600000	IT Communications Technician I
86130	- 4	7400151210	IT Communications Technician II
86130	- 2	7400151220	IT Communications Technician II
86130	+ 8	7400600000	IT Communications Technician II
86131	- 10	7400151210	IT Communications Technician III
86131	- 1	7400151220	IT Communications Technician III

Job Code	+/-	Department ID	Class Title
86131	- 1	7400300000	IT Communications Technician III
86131	+11	7400600000	IT Communications Technician III
86119	- 1	7400300000	IT Supervising Business Systems Analyst
86125	- 1	7400151210	IT Supervising Communications Analyst
86125	+1	7400600000	IT Supervising Communications Analyst
86135	- 2	7400151210	IT Supervising Communications Technician
86135	- 1	7400151220	IT Supervising Communications Technician
86135	+3	7400600000	IT Supervising Communications Technician
86141	- 1	7400300000	Information Technology Officer II
86141	+1	7400600000	Information Technology Officer II
13865	- 1	7400300000	Office Assistant II
13865	+1	7400600000	Office Assistant II
13866	- 1	7400300000	Office Assistant III
76431	- 1	7400300000	Radio Communications Engineer I
76431	- 1	7400151210	Radio Communications Engineer I
76431	+2	7400600000	Radio Communications Engineer I
76429	- 4	7400300000	Radio Communications Engineer II
76429	+3	7400600000	Radio Communications Engineer II
77413	- 1	7400300000	Senior Accountant
77413	+1	7400600000	Senior Accountant
15826	- 4	7400151210	Support Services Technician
15826	+4	7400600000	Support Services Technician

ROLL CALL:

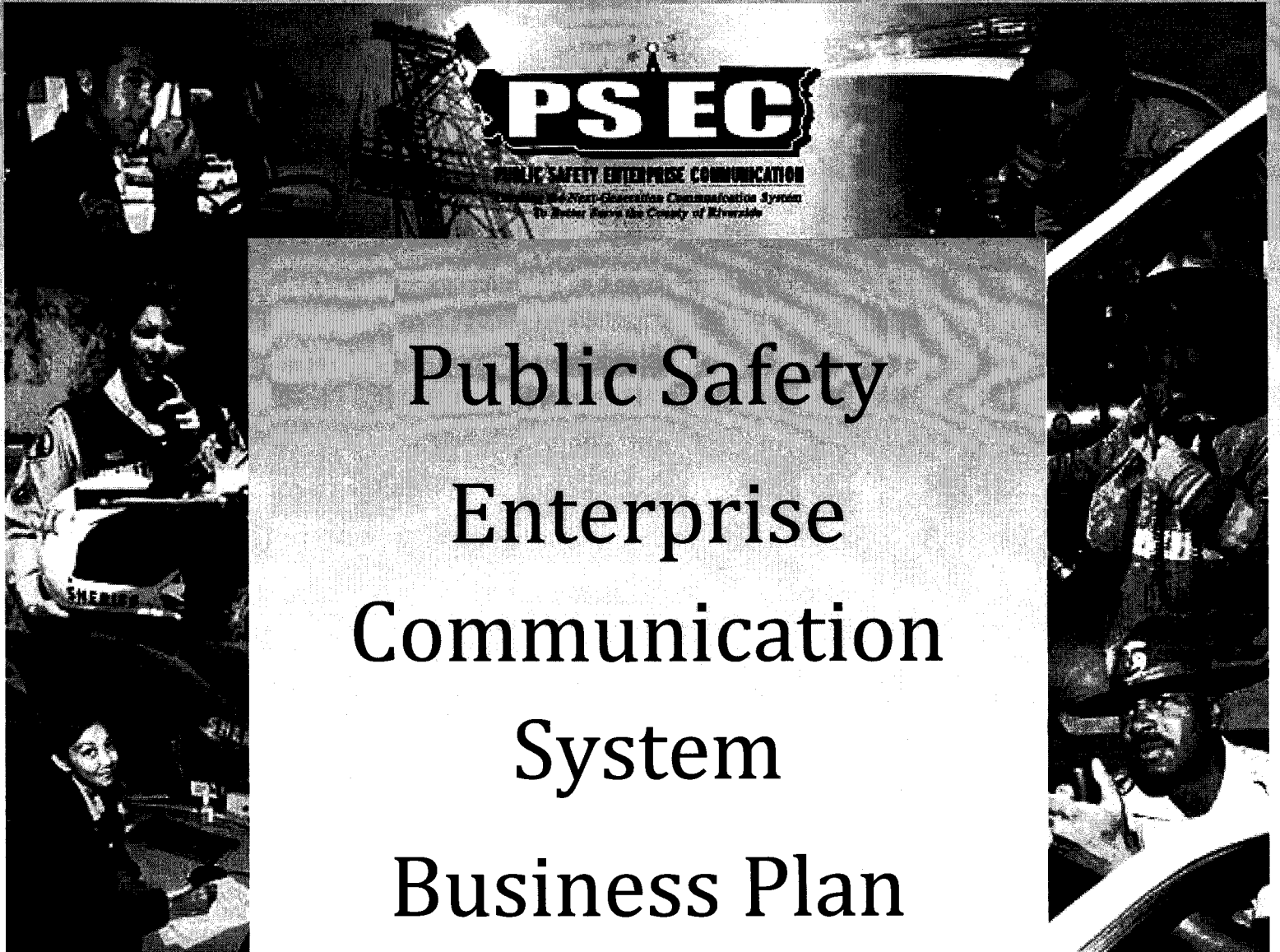
Ayes: Buster, Tavaglione, Stone, Benoit, and Ashley  
 Nays: None  
 Absent: None

The foregoing is certified to be a true copy of a resolution duly adopted by said Board of Supervisors on the date therein set forth.

KECIA HARPER-IHEM, Clerk of said Board

By: \_\_\_\_\_  
 Deputy

/kc  
 10/03/2012  
 440 ResolutionsKC



# Public Safety Enterprise Communication System Business Plan

A cooperative effort among Riverside County



public safety and public service agencies

**Table of Contents**

Executive Summary ..... 3

    Benefits of PSEC..... 5

    Interoperability ..... 6

        What is communication interoperability? ..... 6

    PSEC Key Deliverables ..... 7

    Technology ..... 8

    Client List ..... 9

Marketing Plan ..... 11

Operating Plan ..... 12

    Name & Location..... 12

    Mission Statement..... 12

    Clients ..... 12

    Client Service Standard ..... 12

    Service Levels ..... 13

    Quality Control ..... 13

    Operational Goals..... 13

Organizational Plan..... 15

    Management ..... 15

    Oversight ..... 15

    Staffing..... 15

Financial Plan..... 16

    Summary ..... 16

    Financial Goals..... 16

    Financial Audit..... 16

    Capital Assets..... 16

    Asset Management..... 17

    Operational Expenditures ..... 17

    Revenue..... 17

    Revenue Assumptions..... 18

    Rate Comparison..... 18

    Rates ..... 18

Exhibit A – PSEC Budget..... 19

Exhibit B – PSEC Rates .....	23
Exhibit C – Staffing Plan .....	26
PSEC Organization Chart .....	28
Exhibit D– Governance Board Overview .....	29
Executive Summary .....	29
Introduction .....	30
Mission Statement.....	30
Purpose .....	30
General Duties of Governance Board .....	30
Governance .....	30
Models from Other Counties and States.....	31
Governance Structure .....	31
Exhibit E – Governance Board Policies .....	33
Proper Use of Network Policy .....	34
Maintenance & Support Policy .....	36
Change Control Policy.....	40
Talkgroup Plan Approval Policy .....	43
System Key Control Policy.....	45
Advanced System Key(ASK) Child Key Request Form.....	49
Password Administration Policy .....	50
Access to Administrative Functionality Policy.....	53
Remote Access Policy .....	55
Recommended Form for Electronic Access Request.....	58



# Executive Summary

---

Wireless communication for public safety and public service agencies is an important need essential to rapid and efficient interaction among all public safety organizations. The communication system is a tool that must provide immediate and coordinated assistance in day-to-day missions, task force operations, and mass-casualty incidents. Although local agencies are primarily concerned with communicating with their own agency, they must also work and communicate with other first responder agencies.

The very nature of providing emergency services to the citizens of Riverside County requires reliable, robust interoperable communication. Responding to house fires, auto accidents and other emergency responses involves multi-disciplined agencies providing firefighting, emergency medical treatment and law enforcement services. These responses are most efficient and effective when these agencies can talk to one another using a single radio network.

The success of a major project like public safety communication interoperability in Riverside County will require a process that includes communication, coordination, planning and on-going management. Interoperability requires the commitment of different agencies in the public safety community with responsibilities in a time of crisis. Leadership buy-in is a critical element of this. This process, and a key component of successful interoperability, is *Governance*.

The PSEC Governance Board is the environment in which this collaboration will take place. The main purpose of the PSEC Governance Board will be to provide oversight of the PSEC System and to improve communications and operations among participating public safety and service agencies. Upon implementation of the PSEC System, the Governance Board will be comprised of the existing PSEC Steering Committee members who will work with other agencies to set the standard for countywide collaboration and interoperable communication. Approval of the Governance Board by the Riverside County Board of Supervisors establishes an organizational and management structure for ongoing network administration, operation, and maintenance. The Board will provide a process for admitting other public safety and public service entities to join and participate in the PSEC System and will collaboratively define the allocation of costs associated with the network's operations, maintenance, and enhancement for members, both internal and external to Riverside County.



**THE COMPLETE PSEC SYSTEM DURING STAGING IN SCHAUMBURG**

When an emergency happens in Riverside County, the first responders who provide emergency assistance to the public are members of the County's public safety and public service agencies. The Department of Homeland Security (DHS) Act of 2002, defines emergency response providers as "Federal, State, and local emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities." As a result, non-traditional organizations such as public works and utilities are now part of the public safety sphere.

In earlier decades, individual communities existed in relative isolation, and the need for public safety agencies to intercommunicate was only occasional. Law enforcement, fire departments, and other agencies usually owned and operated their own two-way radio systems. Today, County agencies and municipalities—with their rapid growth rates, dense population centers, and large daily and seasonal population fluctuations—have many common linkages, and public safety officials collaborate and coordinate their efforts on a daily basis.

In 2010, the population of Riverside County was more than 2 million, an increase of almost 42% since 2000. The population increase resulted in public safety and public service agencies increasing their personnel to serve the communities, causing an increase in radio system users. These increases put a strain on the current analog radio system as officers and first responders began requiring communication coverage in areas previously uninhabited. The current analog radio system is outdated, can no longer support the County's population or number of users, and does not effectively meet the changing needs of its emergency responders. The current system requires voice and data communication to take place over the same network and the coverage is lacking in many areas. These inadequacies combine to create safety issues for public safety and public service personnel.

The Public Safety Enterprise Communication (PSEC) System will provide the technology to meet the communication needs of our public safety and public service agencies. Four distinct digital networks will facilitate effective communication among these agencies. Those networks are voice, high performance data, 4.9 GHz broadband data, and microwave.

The PSEC System will be the most feature-rich public safety radio system across the nation. It will enable the County's public safety responders to communicate more efficiently and effectively with each other and with other agencies across the County.

## *Benefits of PSEC*

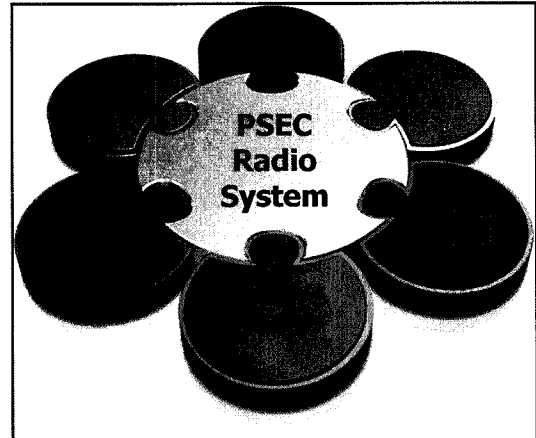
<b>PSEC System</b>	<b>Current M/A-COM System</b>
<ul style="list-style-type: none"> <li>• Built with today's technology, is expandable and can accommodate an increased number of users</li> <li>• Site quantity and location is based on required coverage for Sheriff, the System's largest user, thus providing improved coverage for all users</li> <li>• Guaranteed coverage of high priority buildings and significant improvement in structural coverage</li> <li>• Technology provides an increase in interoperability</li> <li>• Voice and Data have separate networks. Voice communication will use the Interactive Voice and Data (IV&amp;D) network, while data communication will travel over one of 4 different networks – High Performance Data, 4.9 GHz network, data cellular or, as a last resort, the IV&amp;D network</li> <li>• Provides coverage for approximately 90% of the county</li> <li>• Two master sites at each end of the County, can work independently of each other, providing system redundancy</li> <li>• Centralized management to ensure system integrity</li> <li>• Increased channel capacity on 700 MHz band</li> </ul>	<ul style="list-style-type: none"> <li>• Technology is twenty years old and the system has reached/exceeded its capacity limit</li> <li>• Number of sites within the system are based on 1989 demographics</li> <li>• Lack of in-building and structural coverage</li> <li>• Out-of-date technology limits interoperability</li> <li>• Voice and data share the same network and a cellular system is required to augment data communication</li> <li>• Provides coverage for approximately 60% of the County</li> <li>• No redundancy</li> <li>• Lack of centralized management which poses operational risks</li> <li>• Minimal channels on overcrowded 800 MHz band, limiting interoperability with other agencies</li> </ul>

## *Interoperability*

The very nature of providing emergency services to the citizens of Riverside County requires reliable, robust interoperable communication. Responding to house fires, auto accidents and other emergency responses involves multi-disciplined agencies providing firefighting, emergency medical treatment and law enforcement services. These responses are most efficient and effective when these agencies can talk to one another using a single common radio network.

There have been several high profile events nationally, where the lack of interoperable communication has hindered the efforts of public safety. The Columbine School shooting in 1999, the terrorist bomb attack on the Alfred P. Murrah Federal Building in Oklahoma City in 1995 and the terrorist attacks on the World Trade Center in 2001. Additionally, there have been major events in Riverside County where interoperable communication would have improved the efficiency and effectiveness of emergency responders. Examples include the Norco Bank Robbery in 1980, the Esperanza fire in 2006 and the Soboba shootings in May 2008. However, numerous situations happen on practically a daily basis where public safety responders from two or more agencies have a need to communicate with each other.

Public safety agencies in Riverside County currently use a variety of radio technologies, frequencies, and dispatching arrangements. Many of these are working successfully. At the same time, there are issues that must be resolved to improve interoperable communication. The lack of public safety interoperability is a long-standing, complex, and costly problem. One reason is the numerous variables present during situations requiring interoperable communication. Established protocols for event management must be put into place in order for interoperability to work. No two events are the same and therefore cannot be responded to in the same way. While several government programs have made great strides in addressing these issues, much of this work has been disconnected, fragmented, and often conflicted. The SAFECOM program was established in 2001 in an effort to coordinate the various Federal initiatives and eliminate the fragmentation and conflicts.



The PSEC Radio System provides interoperable communication, enabling County agencies to talk to each other when the need arises.

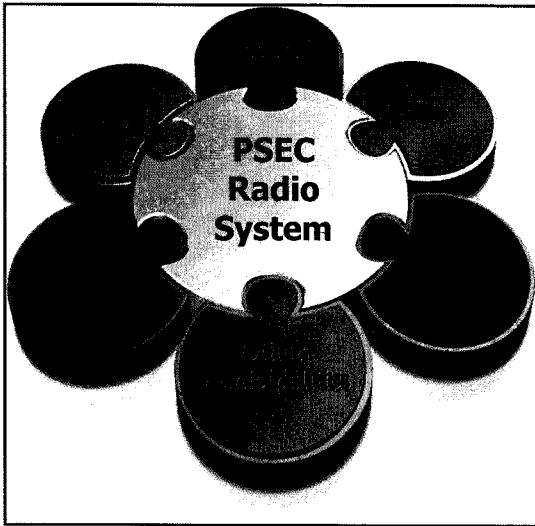
### *What is communication interoperability?*

In general, communication interoperability refers to the ability of emergency responders to work seamlessly with other systems or products without any special effort. For example, when communication systems are interoperable, police and firefighters responding to a routine incident can talk to each other to coordinate efforts. SAFECOM's definition states:

Communication interoperability is the ability of public safety practitioners to talk to one another across disciplines and jurisdictions via radio communication systems, exchanging voice and/or data with one another on demand, in real time, when needed and when authorized.

Communication interoperability also makes it possible for emergency response agencies responding to catastrophic accidents or disasters to work effectively together. Finally, it allows emergency

response personnel to maximize resources in planning for major predictable events such as the Super Bowl, a presidential inauguration, or for disaster relief and recovery efforts.



The PSEC Radio System provides interoperable communication, enabling County agencies to talk to other agencies when the need arises.

Ideally, interoperability is achieved by using a single, unified radio system, serving the entire public safety community. Such a system provides automatic interoperability, not limited by different frequency bands or even by manufacturer proprietary protocols in the same frequency band. A single, unified system serving the entire public safety community would achieve the best level of interoperability, provide the most features, and be the simplest to operate. A shared system can take many forms, but normally includes a common infrastructure and technology.

Note that “interoperability” encompasses not only technology, but also, most importantly, governance, standard operating procedures, training and exercise, and usage, and exists along a continuum. PSEC will use the SAFECOM Interoperability Continuum as the tool to define the county’s interoperability status. The Continuum also provides a dramatic example of the various states of interoperability, from simply exchanging radios from one system to another, to a standards-based shared system.

## *PSEC Key Deliverables*

The main deliverable of the PSEC Project is to deliver a system that provides operability for all current users. The system was designed to meet the needs of the current radio users with the ability to expand to meet the regional needs of all County departments as well as other public safety and public service agencies throughout Riverside County. The implementation of the PSEC System will provide a county-wide voice and data radio communication system ensuring that emergency responders have the tools to communicate quickly and effectively, each and every time they call for assistance, and to provide a communication system that promotes interoperability between public safety agencies.

**Regional Network** – There are public safety agencies throughout Riverside County that have reason to communicate with each other on a weekly and sometimes daily basis. Different public safety agencies respond together to requests for assistance such as traffic collisions, house fires and multi-agency efforts. Having a regional network would enable those agencies to communicate more efficiently on an ongoing basis.

**Interoperability** – Interoperability is a priority concern in public safety today. Effective interoperability is difficult within the fragmented systems currently in place in Riverside County. To effectively reach full interoperability, collaboration is required between the participating agencies. The PSEC System is the first step in that process.

**Coverage Density** – Coverage depends upon whether a mobile (or portable) radio is within range of a receiver site, or the transmitter is within range of the mobile (or portable) radio. Coverage refers to the area surrounding a tower site within which a mobile or portable can send or receive transmissions. Mobile radios are more powerful than portables, so coverage from a given site is significantly greater

for mobiles. The PSEC System provides mobile coverage at approximately 95% across the County, with portable coverage averaging a little less than 90%. Overall, the PSEC System will provide coverage over 90% of the County, including areas not currently covered, as well as 95% transmission reliability, a significant improvement over the current analog system. There are 21 ASTRO-25 non-simulcast sites that the Sheriff's Aviation unit will use. Although those sites can also be used by other users, the primary function is for the Aviation units.

The PSEC System covers those areas accessed by emergency first responders, while the remaining areas are inaccessible due to terrain and topography issues. Through the use of aviation communication, should an emergency responder be required to go into an inaccessible area, they will still have communication with the aviation unit through the use of direct channels.

Reliability – the PSEC system was designed to provide 95% reliability for the end users. This means for every 100-voice transmissions, only 5 may be delayed.

Redundancy – there is redundant equipment at each site, including redundant power backups, and redundant microwave paths. The System also includes two master sites, one at each end of the county in the event of a site failure in the central part of the county.

## *Technology*

The system was designed with current Project 25 technology. Project 25 (P25) is a set of standards produced through the joint efforts of the Association of Public Safety Communications Officials International (APCO), the National Association of State Telecommunications Directors (NASTD), selected federal agencies and the National Communications System (NCS), and standardized under the Telecommunications Industry Association (TIA). The P25 standards are a collaborative effort by public safety agencies and manufacturers to address the issues with emergency communication systems and to ensure that all manufacturer's two-way radios are interoperable. The goal of P25 is to enable public safety responders to communicate with each other and, thus, achieve enhanced coordination, timely response, and efficient and effective use of communication equipment.

The system is comprised of separate voice and data networks. Depending upon several variables, the data traffic will travel over one of the four avenues – the High Performance Data (HPD) network, the 4.9 GHz broadband data network, the data cellular network or, as a last resort, the Interactive Voice and Data (IV&D) network.

The County currently has an intercom connection that allows the Riverside County Sheriff Department Dispatch center to connect with several other dispatch centers, such as San Bernardino and San Diego. Once the surrounding counties

### ***Top 5 Benefits of PSEC***

---

***Coverage - Approximately 86% of the county is covered; coverage has been increased in remote areas; For some agencies, they could have 100% coverage in their jurisdictions (e.g. local police agencies)***

---

***Interoperability – ability to talk to other agencies when the need arises***

---

***Latest Technology – Standards-based P25 capable***

---

***Redundancy / Reliability – two master sites, redundant equipment at each communication site and 95% reliability***

---

***Voice and data networks – Voice and data communication takes place over separate networks; data can travel over one of 4 different paths, increasing efficiency.***

upgrade their radio systems to P25 capable, system keys can be exchanged, which will allow Riverside County radios to work on their systems and vice versa.

## *Client List*

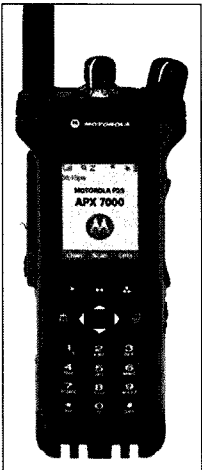
The clients on the current analog system, will continue to have services provided by the RCIT-PSEC group after the new PSEC System is implemented.

### Current Clients

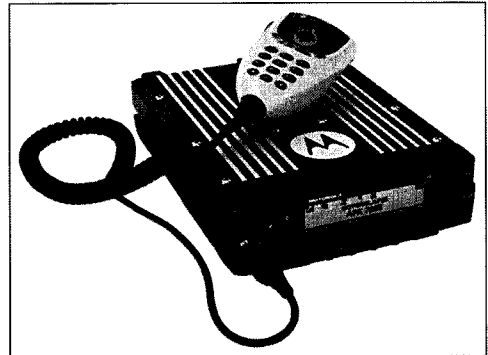
City of Meniffee (City Services)	BLM
District Attorney	Lake Hemet
Riverside County Parks	Union Pacific Railroad
City of Canyon Lake (City Services)	FBI
County Health Agency – Animal Services	County Health Agency – Bio-terrorism
County Health Agency–Emergency Management Services	County Health Agency – Hospitals
Mental Health	City of Moreno Valley (City Services)
CDF/County Fire Maintenance	CDF/County Fire Law Enforcement
Riverside County Waste Management	City of Palm Desert (City Services)
City of La Quinta (City Services)	City of Rancho Mirage (City Services)
City of Perris (City Services)	City of San Jacinto (City Services)
Riverside County Department of Public Social Services	

### Riverside County Sheriff providing services to the County and contract cities of:

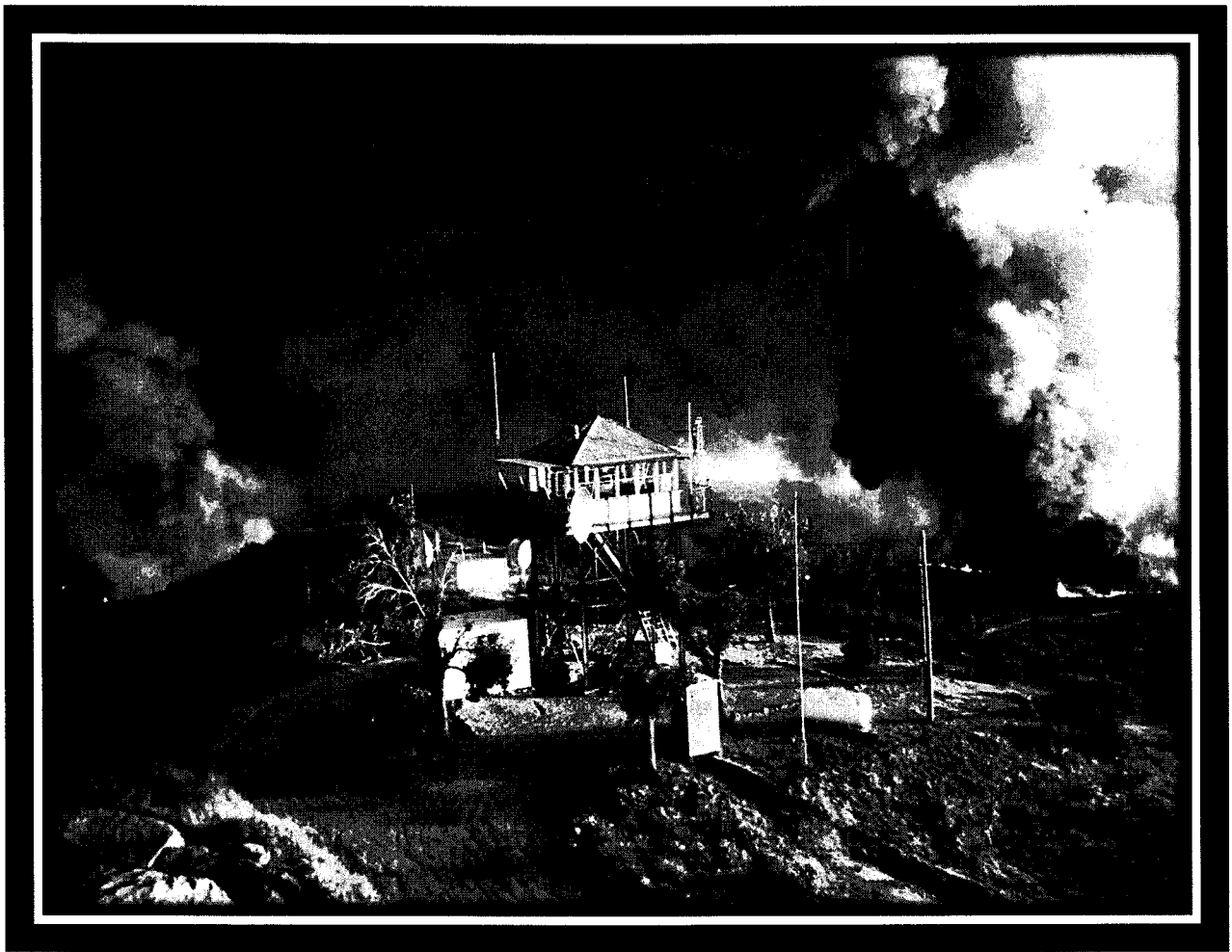
Calimesa	Canyon Lake	Coachella
Eastvale	Indian Wells	Jurupa Valley
Lake Elsinore	La Quinta	Meniffee
Moreno Valley	Norco	Palm Desert
Perris	Rancho Mirage	San Jacinto
Temecula	Wildomar	Morongo Indian Reservation



APX 7000  
Dual Display  
Portable Radio



APX 7500 Mobile Radio



MOUNTAIN TOP COMMUNICATION SITE IN THE MIDST OF A FIRE



# Marketing Plan

---

The Public Safety Enterprise Communication System (PSEC) is expandable and can accommodate the regional needs of all county department radio users as well as other public safety and public service agencies throughout the county; it is important that these agencies are made aware of the system's capabilities and the potential to participate as a user. Key messages about the PSEC System are its capabilities to improve safety and its potential for cost savings for each user. The following marketing and media plans are proposed for the purpose of creating awareness of the County of Riverside's new PSEC System among other county departments, non-county governmental and quasi-governmental agencies.

The marketing and media plans will outline tools that will assist in informing the public and all agencies about PSEC's potential through staff presentations, advertising and media coverage. Presenting the information in person to potential clients will be a key strategy for PSEC staff, as will media relations and editorials in local newspapers and industry magazines. As additional users take advantage of the PSEC system the revenue generated will offset the PSEC operating costs, while dramatically decreasing expenditures for all participating agencies.

# Operating Plan

---

## *Name & Location*

The RCIT Communication Solution Division under the direction of the Governance Board, will provide services under the name Public Safety Enterprise Communication System. This system will provide wireless and data communication services to emergency and first responders throughout the County of Riverside. The PSEC System offices will be maintained at 7195 Alessandro Boulevard, in the City of Riverside.

## *Mission Statement*

The mission of the Public Safety Enterprise Communication System is to provide and maintain an effective voice and data communication network for the Riverside County public safety and public service agencies, component units of the County, and other state and federal agencies.



MEMBERS OF THE VEHICLE INSTALL TEAM

## *Clients*

There are twenty-three agencies on the current analog system. Those clients will be the initial users of the PSEC System. The PSEC team has met with eleven other agencies to determine their operational needs and to develop a transition plan to identify how their agency will transition after the PSEC System is implemented.

Use of the PSEC System is limited to public safety and public service agencies, as defined by the Department of Homeland Security. Primary clients will consist of direct users of the voice and data systems. Secondary clients are agencies such as public service agencies with their own radio systems, which use Riverside County communication sites to house their equipment.

The PSEC Project team has met with several public safety and public service agencies to determine their communication needs and to identify how the PSEC System can meet those needs. The team is gathering information such as the number of users and how they currently do business. This information, as well as other specific data, is analyzed to provide prospective agencies with detailed information on how the PSEC System can meet their organizational needs.

## *Client Service Standard*

As a public safety communication system, it is imperative the system operate twenty-four hours per day, seven days per week, and three hundred sixty-five days per year (24/7/365). Therefore, the PSEC System contains redundant components to prevent system failure in an outage situation thus guaranteeing operability and safety for users.

## *Service Levels*

Each agency will identify their service level expectations as Must Have and Options. The PSEC Project team will develop an agreement with each agency identifying how the detailed service levels will be met for the must have requirements and how best to provide the options, if available.

## *Quality Control*

The System includes several tools that will be used to monitor, troubleshoot, and manage the PSEC System. Many of these tools provide remote management so monitoring and troubleshooting is more efficient for support staff.

The System includes reporting software that will allow support staff to generate historical reports related to system usage and system alarms. A specialized server will collect, prepare, and store the information obtained through various interfaces. The information collected will result in approximately 30 different reports providing the status of all aspects of the System.

The System also includes a performance monitoring tool that can provide a graphical representation of network statistics. This tool InfoVista interfaces with, and gathers data from, multiple ASTRO 25 system network devices. The primary function of this tool is to provide HPD statistical information, but also provided is statistical information for the voice system.

## *Operational Goals*

The PSEC Project team is developing a five-year plan that includes immediate (1 year or less), short-term (1-5 years), and long-term (5 or more years) goals.

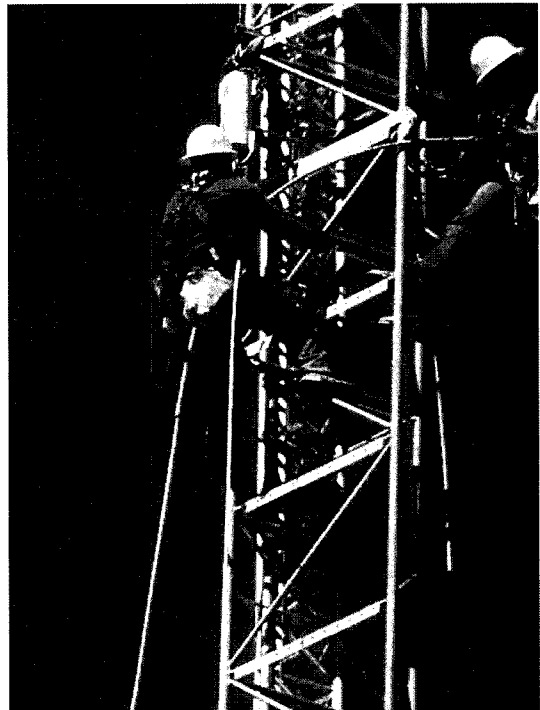
### Immediate

The security of the sites is of utmost importance and therefore, the PSEC team is developing security options for each site. Some sites are remote, while others are located within industrial areas. Rather than creating a blanket security plan, each site is being analyzed to determine the criticality to the system, the number of connections to other sites, and the ease of access to the site.

### Short Term

During the first two years after the PSEC System is implemented, all agencies are required to use the Motorola APX subscriber unit (mobile or portable). During this time, the engineering team will analyze the use of other manufacturer's P25 compliant subscriber units on the PSEC System. The analysis will include information such as impact to the system, acceptable equipment specifications and other implications as identified.

Upgrade to P25 Phase II – The P25 Phase II Standard was approved in November 2010. To transition to Phase II, requires a hardware & software upgrade. The upgrade will take the PSEC System from a proprietary system to an open standards-based system.



TOWER CLIMBERS INSTALLING EQUIPMENT

Northern microwave route – The current microwave system contains a single point of failure at one of the centrally located microwave sites. Should a serious outage occur, the loss of this site will disconnect the east end of the county from the west end of the county. Although the PSEC System is designed with two master sites to operate independently, should this happen, County Fire would be unable to connect with their main dispatch center in the western portion of the county.

Upgrade channel banks for microwave – The channel banks for the microwave system were installed in 1987 and have been in service for 25 years. The company was sold 8 years ago and, as a result, repairs for the product will eventually become unattainable. There is currently no technical support for much of the equipment.

Construction of the Palo Verde site – The Palo Verde site has had significant acquisition issues as a result of other projects within the County of Riverside. The team continues to work on the acquisition process to incorporate this site into the PSEC System.

### Long Term

LTE – Long Term Evolution is a wireless broadband technology standard that uses an “all-IP” architecture where everything is handled as data, similar to the internet. It provides significantly faster upload and download rates. LTE will support mixed data, voice, video and messaging traffic.

Video Streaming – Video streaming encompasses a broad range of use cases. This communication tool can be used to provide incident or other pertinent video between vehicles and between agencies (where capable).

# Organizational Plan

---

## *Management*

The Riverside County Information Technology, Communication Solution Division Senior Manager will be responsible for the day-to-day operations of the PSEC System, with direct oversight from the Assistant Chief Information Officer.

## *Oversight*

PSEC was designed and built to provide a regional communication network for all public safety and public service agencies throughout Riverside County. Part of managing a regional system requires that a well-defined and structured Governance Board be in place to empower the efforts behind the system to encourage the cooperation of the participating agencies. An overview of the proposed Governance Board can be found in Exhibit D – Governance Board Overview.

Fundamental assumptions underlying the concept of a countywide public safety radio system are shared benefits and funding. The experience of other multi-jurisdictional systems clearly demonstrates that joint governance is the key to general acceptance and success. Although the County needs to provide leadership in starting the process, genuine shared governance must be a commitment.

Two apparently conflicting objectives of a consolidated countywide radio system are the requirements to preserve individual agency control and identity while also participating in a common communication medium. However, within a shared system, users may continue to maintain autonomy and control over their radio communication needs and functionality. Initially, the Governance Board would take on the development of the shared view of the long-term integrated System. The Board would also discuss and resolve operational procedures and shared funding mechanisms.

County and municipal public safety officials are the ideal candidates for membership in the Governance Board. The proposed structure and details of the PSEC Governance Board will be presented to the Board of Supervisors under a separate Form 11.

## *Staffing*

Forty-one (41) dedicated staff positions will be required to support the PSEC Project once in production and operational, as well as support from other Bureaus within RCIT. They include an ongoing commitment from the County's Public Safety partners, Sheriff and Fire. The positions are outlined in Exhibit C – Staffing Plan.

# Financial Plan

---

## *Summary*

The Governance Board is responsible for approving and developing the rates for the PSEC System. The RCIT Communication Solution Division will support and maintain the PSEC System as an Internal Service Fund (ISF) as a sub-organization of RCIT. This ISF model exists for the current legacy system and will provide services to other departments and agencies on a cost-reimbursement basis. The goal of PSEC is to measure the full cost of providing its service and recovering those costs through support and system usage fees. As a project, the PSEC system was reliant on general funds, and after implementation of the system, the vision is to move from that dependency to reliance on service revenues to establish financial stability. Continuing as an ISF will enable the division to consider the total economic costs, provide for on-going capital needs and provide rate stability, in support of the objectives set forth by the Board.

## *Financial Goals*

During the annual budgeting process, the PSEC team will review the existing budget and recommend financial goals to make the system cost effective for all clients and to maintain financial sustainability for the System. Goals will be identified as immediate (less than 1 year), short-term (1-5 years) and long-term (5 or more years). The Executive Office has established a mid-term goal for the PSEC team to have a plan developed that will transfer the capital assets to the PSEC Budget and develop an infrastructure equipment replacement plan. The PSEC System budget will be reviewed and approved by the PSEC Governance Board. The PSEC System Budget will be submitted as part of the overall RCIT budget.

## *Financial Audit*

RCIT will establish and maintain the accounting systems according to the generally accepted principles and standards of the Government Accounting Standards Board (GASB) and the National Committee on Governmental Accounting, in accordance with the Riverside County Auditor-Controller's Office. Financial systems will be maintained to monitor expenditures and revenue on a monthly basis with a thorough analysis and adjustment (if required). The financial goals will guide the development of the budget and action plan for the upcoming year.

The documented goals will be provided to the Board of Supervisors as part of the budget approval process. The goals will include detailed information about required personnel, operational costs, expected revenue, and anticipated capital expenditures.

## *Capital Assets*

The Executive Office will maintain all assets and depreciation during the first three years of operation. During that time, the RCIT Communication Solution Division Senior Manager will work with the PSEC Governance Board to establish an asset replacement plan. The goal is to complete the plan by the end of year five.

Agencies will be responsible for the asset management of their subscriber equipment, which will be obtained through either a purchase or lease program directly through Motorola. Each agency will be responsible for establishing an equipment replacement plan.

## *Asset Management*

The RCIT Communication Solution Division will be responsible for asset management of all system equipment that makes up the infrastructure of the voice and data communication systems, using RCIT enterprise reporting and tracking systems.

## *Operational Expenditures*

Because the PSEC System is a public safety communication System, maintaining the system is imperative to provide near-zero interruptions to the system and its end-users. In the first two (2) years, the anticipated maintenance cost for infrastructure equipment is expected to be minimal. Starting in year three, additional operational expenditures, such as diesel generator rebuilds and structural integrity inspections on the towers, will be required.

The shelters and associated equipment will require maintenance. Examples of regular, monthly site maintenance includes, but is not limited to, fueling of diesel and propane generators, HVAC service, and weed abatement. Every three years, diesel generators must be rebuilt.

The PSEC System consists of existing and new communication towers. The existing towers have been in place several years and should be inspected for structural integrity every year. Since the new towers have been built in accordance with the newest engineering and structural requirements, inspections should take place every two years. The County currently has two awarded vendors that are certified to conduct tower inspections. The County can establish a rotating schedule with the vendors to ensure tower inspections occur within the established timeframes.

Additional operational expenditures include fees associated with environmental compliance. Each year, permits from the Air Quality Management District (AQMD) and Riverside County Environmental Health require renewal fees.

## *Revenue*

As services and service levels are determined by each agency, the question of funding those services arises. Revenue will be generated through license agreements with non-County governmental and quasi-governmental (federal, state, and municipal) agencies who wish to install their agency's communication equipment in the County's existing communication shelters. Additional revenue will come from county agencies through MOUs (Memorandums of Understanding) for participation on the communication system. Services levels necessary for agencies using the voice or one, or more, of the data networks will be established.

Monthly system usage fees are calculated based upon the number of talk groups and the number of communication cells of which each agency takes advantage.

Monthly fees for occupying space within the communication shelters are calculated based upon the space each agency's equipment occupies within the equipment racks as well as the space equipment occupies upon the tower. Equipment rack fees are based on  $\frac{1}{4}$  space intervals, or any portion thereof, used. A fee for tower space is new to RCIT and was determined based upon best practices by surrounding counties.

The fees associated with space in the communication shelters will be allocated to the cost of maintaining the shelter and enclosed equipment.

## *Revenue Assumptions*

The purpose of revenue is to offset the costs for all clients and help maintain and grow the PSEC System infrastructure as required. As additional agencies take advantage of the PSEC System, the overall cost to all participants is lowered or future enhancements funded.

- Revenue will be generated from participating agencies on the radio system based upon the number of cells and talkgroups used by each agency. As the number of participating agencies increases, the cost of the overall system should decrease, thus decreasing each participating agency's monthly expenditures.
- The rates for non-County Agencies will be negotiated individually with each department.

## *Rate Comparison*

Riverside County is geographically over seven times larger than Orange County and has a much more diverse and challenging terrain to cover by radio frequency. The Orange County system has full participation in the system by all County Radio System users and the 34 incorporated Cities. Riverside County will have the initial participation of 3600 County voice users and 900 Fire data users. No cities in Riverside County are participating in the system except through contract with the Riverside Sheriff Department. Rates have been developed to allow other government agencies to join the system. The Orange County system has over five times the amount of voice subscribers than the Riverside County system including participation of 100% of all Law and Fire users.

Orange County Fire agencies like the Orange County Fire Authority, Brea, Laguna Beach, Santa Ana and Metro Net (a seven city Anaheim, Fountain Valley, Fullerton, Garden Grove, Huntington Beach, Newport Beach, and Orange joint power agreement) maintain their own private data systems/utilize cellular services. The Orange County Sheriff's Department utilizes a cellular data system for its mobile data needs.

Orange County has approximately 81 800 MHz frequencies that are 25 kHz wide. Riverside County has 204 7.25 kHz 700 MHz frequencies.

The Orange CCCS Radio system was paid for up front based on a cost sharing formula across all participating agencies. Ongoing backbone maintenance costs are recovered based on a similar formula. Much of the costs of the initial system were subscribers while much of the Riverside initial costs are remote sites and backbone equipment.

Riverside County has 45 more radio sites to maintain than Orange County to provide Public Safety Grade Communication. Comparing Riverside and Orange County side-by-side, we see that Riverside County's system is more extensive.

## *Rates*

The rates for the PSEC System are described in the proposed Rate Sheet, attached as Exhibit B.



# Exhibit A – PSEC Budget

				<b>Base Line Enterprise Budget</b>							
				4.9 Data	Radio						
				Modem	HPD	Voice & Inter Op	MDC	Vehicle	Site	Microwave	Base line budget backbone
Position/Title		Requested	Existing	Addition							
<b>Appropriation 1 - Salaries and Benefits</b>											
Full time	Office Assistant II	0	2		-	-	-	-	-	-	-
Full time	Senior Accountant	0	1		-	-	-	-	-	-	-
Full time	Business System Analyst (sup)	0	1	0	-	-	-	-	-	-	-
Full time	Administrative Services Analyst II	0	1		-	-	-	-	-	-	-
	<b>Total Administrative Salaries and Benefits</b>	<b>0</b>	<b>5</b>	<b>0</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>
Full time	Information Officer II	1	2		11,886	11,886	57,052	11,886	21,394	30,903	26,149
Full time	Warehouse	0	0		-	-	-	-	-	-	-
Full time	Radio Communication Engineer II	3	3	0	-	157,244	316,284	-	-	-	-
Full time	Radio Communication Engineer I	2	1	1	21,268	21,268	21,268	21,268	21,268	-	156,933
New	IT Supervisor Com Analyst	1	0	1	35,538	35,538	-	-	-	71,077	-
Full time	IT Communication Analyst III	3	4		135,130	130,723	-	-	-	135,130	-
Full time	IT Supv Communication Tech	3	3		23,126	23,126	46,253	29,585	88,754	29,585	88,754
Full time	IT Communication Tech II	6	6		20,983	20,983	84,433	110,885	110,885	-	169,595
New	IT Communication Tech II Vacant	2	0	2	-	-	-	-	-	122,340	-
New	Support Services Tech	4	0	4	-	-	-	-	-	197,067	-
New	IT Comm Tech 1	1	0	1	3,775	3,775	18,122	3,775	6,796	9,816	8,306
Full time	IT Communication Tech III	11	11		104,351	102,013	595,287	58,395	274,692	-	54,481
	Overtime				8,993	18,952	81,171	-	25,917	17,497	17,343
	Standby Pay				-	52,658	48,033	-	6,482	28,602	20,601
	Administrative Leave Buy out				-	-	1,625	-	1,625	-	1,625
	Flex Benefits increase				920	1,264	3,277	1,127	1,890	2,740	2,186
	Advance Grade Recognition				1,319	1,319	1,833	319	875	2,431	1,903
517000	Workers Comp Insurance										1,072
	<b>Total Eng. And Tech. Salaries and Benefits</b>	<b>37</b>	<b>30</b>	<b>9</b>	<b>364,952</b>	<b>578,169</b>	<b>1,269,527</b>	<b>235,794</b>	<b>557,815</b>	<b>642,016</b>	<b>543,787</b>
	<b>Total Appropriation 1 (Salaries and Benefits)</b>	<b>37</b>	<b>35</b>	<b>9</b>	<b>367,191</b>	<b>580,752</b>	<b>1,274,637</b>	<b>237,240</b>	<b>560,580</b>	<b>647,187</b>	<b>547,876</b>

## Base Line Enterprise Budget

				4.9 Data						Base line budget backbone	
				Radio							
				Modem	HPD	Voice & Inter Op	MDC	Vehicle	Site		Microwave
<b>Appropriation 2 - Supplies and Services</b>											
520220	Battery Recycle Ecology Control Industries Inc			-	-	-	-	500	-	-	500
520220	Battery Zone			-	-	-	-	200	-	-	200
520220	Black Box - Specialized Cabling			-	-	-	4,000	-	-	-	4,000
520220	Conventional UPS Battery Maintenance			-	-	10,000	-	-	-	-	10,000
520220	Dailey Wells Conventional parts			-	-	10,000	-	-	-	-	10,000
520220	Misc for site work			35	535	5,667	35	63	90	76	6,500
520220	Misc for Radio work			-	-	6,100	-	-	-	-	6,100
520220	First Communication Radio Part Blanket PO			-	-	1,000	-	-	-	-	1,000
520220	Motorola Radio License Fee			-	2,500	2,500	-	-	-	-	5,000
520220	Software Upgrade Agreement II			-	586,000	586,000	-	-	-	-	1,172,000
520220	Blanket PO - Radio Parts			-	2,500	2,500	-	-	5,000	-	10,000
520220	3rd Party for Nice Maintenance			-	-	40,000	-	-	-	-	40,000
520220	3rd Party for Genesis Maintenance			-	-	79,780	-	-	-	-	79,780
520220	3rd Party for Radio IP			-	-	55,080	-	-	-	-	55,080
520220	Spare Antenna Installation Parts			-	-	6,025	-	-	-	-	6,025
520220	GPS Symmetricom Repairs			-	-	5,000	-	-	-	-	5,000
520230	Cellular Phone			486	10,086	11,933	486	875	7,264	8,069	39,200
520260	Verizon Enterprise Network Infrastructure Circuits			143,897	-	-	-	-	-	-	143,897
520260	4.9 Costs			630,471	-	-	-	-	-	-	630,471
520260	Master Site IV&D Circuit Cost Alessandro to Blythe			-	3,954	3,954	-	-	-	-	7,907
520260	Master Site IV&D Circuit Cost Blythe to Alessandro			-	20,295	20,295	-	-	-	-	40,590
520260	Fire Network Infrastructure			82,821	-	-	-	-	-	-	82,821
520815	Cleaning and Custodial Supp			67	1,037	323	67	121	175	148	1,940
521340	Maint - Communication Equipment			80,658	-	5,162	-	-	-	1,600	87,420
521360	Maint - Computer Equipment			-	9,450	9,450	-	-	-	-	18,900
521380	Maint - Copier Machine			104	104	500	104	188	271	229	1,500
521460	Maint-Microwave Equipment			-	-	-	-	-	-	214,000	214,000
521580	Maint- Radio Elec Equipment			1,000	-	5,600	13,330	25,480	-	-	45,410
521640	Maint- Software			2,808	2,808	28,478	2,808	5,054	7,301	6,178	55,435
522310	Maint - Building and Improvement			-	-	-	-	-	-	-	-
522310	Alessandro ground maintenance Form II 33.K 2/7/2012			6,653	6,653	31,936	6,653	11,976	17,299	14,637	95,809
522310	3 site Radio Project Debt Services			-	-	-	-	-	290,295	-	290,295
522310	Santa Rosa General PM			-	-	-	-	-	1,000	-	1,000
522310	Amerigas - Propane Tank Rentals			-	-	-	-	-	1,000	-	1,000
522310	Eaton - Powerware Service Contract			-	-	-	-	-	15,000	-	15,000
522310	Remote Site HVAC Emergency Repairs			-	-	-	-	-	13,000	-	13,000
522310	Remote Site Road Repairs			-	-	-	-	-	10,000	-	10,000
522310	County Facility Management- Form 5 repairs (Radio Site)			-	-	-	-	-	18,000	-	18,000
522310	Cutting lock and safe - General locksmith services			-	-	-	-	-	1,800	-	1,800

## Base Line Enterprise Budget

		4.9 Data							Base line budget backbone
		Radio							
		Modem	HPD	Voice & Inter Op	MDC	Vehicle	Site	Microwave	
<b>Appropriation 2 - Supplies and Services (continued)</b>									
522310	Fire Extinguisher Recharged	-	-	-	-	-	1,700	-	1,700
522310	Generator Engine Parts	-	-	-	-	-	2,400	-	2,400
522310	Riverside County Fire - Brush Clearance Services, Six Sites	-	-	-	-	-	35,000	-	35,000
522310	Tower Maintenance & Repair	-	-	-	-	-	20,000	-	20,000
522310	Physical Security	-	-	-	-	-	50,000	-	50,000
522310	Environmental Health Annual Fees	-	-	-	-	-	80,000	-	80,000
522310	Tower Consultant	-	-	-	-	-	20,000	-	20,000
522310	Microwave Site Routers MWOB	-	-	-	-	-	28,304	-	28,304
523100	Membership	250	250	1,800	250	450	900	2,050	5,950
523220	License and Permit	-	-	-	-	-	-	-	-
523220	AQMD Annual Permit and Emission Fee	-	-	-	-	-	31,775	-	31,775
523220	EPA Number Fee	-	-	-	-	-	250	-	250
523220	Annual Google Earth Pro	75	75	358	75	134	194	164	1,075
523640	Computer Equipment-Non Fixed Assets	306	306	1,467	306	550	794	12,772	16,500
523660	Computer Supplies	694	694	3,333	694	1,250	1,806	1,528	10,000
523700	Office Supplies	347	347	1,667	347	625	903	764	5,000
523760	Postage and Mailing	243	243	1,167	243	438	632	535	3,500
523840	Computer Equipment Software	347	347	1,667	347	625	903	764	5,000
524740	County Support Services COWCAP	6,597	6,597	31,667	6,597	11,875	17,153	14,514	95,000
525020	Legal Services	2,083	2,083	10,000	2,083	3,750	5,417	4,583	30,000
522310	Comm. Site Generator Services	-	-	-	-	-	394,425	-	394,425
525440	Professional services	-	-	-	-	-	-	-	-
525440	Contingency	-	-	221,592	-	-	-	-	221,592
525440	Sheriff, Fire, and EDA (FormV) Services	27,063	27,063	129,902	27,063	48,713	103,363	59,538	422,705
525440	Internal Grant Writing	1,736	1,736	8,333	1,736	3,125	4,514	3,819	25,000
525440	UPS Maintenance Contract	-	-	-	-	-	33,000	-	33,000
526710	Rent - Lease Land	-	-	-	-	-	756,003	-	756,003
526960	Safety Boots	139	139	667	139	250	361	306	2,000
526960	Safety Items	347	347	1,667	347	625	903	764	5,000
527100	Fuel	-	-	-	-	-	1,321,835	-	1,321,835
527840	Training - Education/Tuition	256	256	1,867	56	1,100	1,344	11,522	16,400
527880	Training - Other	2,083	2,083	10,000	2,083	3,750	5,417	4,583	30,000
528920	Car Pool Expense	76	37,276	37,567	76	18,738	68,199	80,863	242,795
528960	Lodging	139	139	667	139	250	361	306	2,000
528980	Meals	35	35	167	35	63	90	76	500
529540	Utilities (Commercial Power)	-	-	-	-	-	850,000	-	850,000
<b>Total Appropriation II</b>		<b>991,817</b>	<b>725,939</b>	<b>1,392,835</b>	<b>70,100</b>	<b>140,767</b>	<b>4,225,440</b>	<b>444,390</b>	<b>7,991,289</b>

## Base Line Enterprise Budget

				4.9 Data	Radio						Base line budget backbone	
				Modem	HPD	Voice & Inter Op	MDC	Vehicle	Site	Microwave		
<b>Appropriation 3 - Other Services</b>												
532600	Capital Lease			-	-	1,892,166	-	5,533	-	244,839	2,142,538	
533720	Cap-Lease Purch Interest			-	-	715,284	-	470	-	4,023	719,777	
535560	Depreciation			-	-	204,580	-	-	4,480	47,397	256,457	
533720	Microwave Site Router - CISCO			-	-	-	-	-	294,979	-	294,979	
<b>Total Appropriation III</b>				-	-	<b>2,812,030</b>	-	<b>6,003</b>	<b>299,459</b>	<b>296,259</b>	<b>3,413,751</b>	
<b>Appropriation 4 - Fixed Assets</b>												
546160	Equipment Other			-	-	-	-	-	-	-	-	
546060	Equipment - Communication			-	-	175,000	-	-	-	-	175,000	
<b>Total Appropriation IV</b>				-	-	<b>175,000</b>	-	-	-	-	<b>175,000</b>	
<b>Site Cost (cost allocated to HPD, Voice and Microwave)</b>					<b>372,475</b>	<b>4,099,896</b>			<b>(4,679,875)</b>	<b>207,504</b>	<b>(0)</b>	
<b>Microwave</b>						<b>918,187</b>				<b>(918,187)</b>	<b>-</b>	
<b>Total Expenditure for FY12/13</b>				<b>1,359,009</b>	<b>1,679,166</b>	<b>10,672,585</b>	<b>307,341</b>	<b>707,350</b>	<b>492,211</b>	<b>577,842</b>	<b>15,796,919</b>	
<b>Revenue to cover some of the cost (site cost, MDC, and Vehicle)</b>					<b>(26,179)</b>	<b>(286,364)</b>	<b>(96,864)</b>	<b>(290,592)</b>	<b>(492,211)</b>	<b>(118,072)</b>	<b>(1,310,282)</b>	
<b>Base Line Budget Grand Total After The Revenue:</b>				<b>1,359,009</b>	<b>1,652,987</b>	<b>10,386,221</b>	<b>210,477</b>	<b>416,758</b>	<b>0</b>	<b>459,770</b>	<b>14,486,637</b>	
1,295	Modem (390 for Fire and 905 for Sheriff)			82.12	108.05							
4,083	County Radio					217.83						
892	Mobile Data Computer						28.71					
4,975	Mile Analog Forecasted Unit Conventional (Sheriff Only)								9.68			

# Exhibit B – PSEC Rates

Operations					
Service Description	Definition	FY 12/13 Rate	Unit	Budget Account	Account Description
4.9 by Modem	Monthly charge per modem	\$82.12	Per Modem per Month	520260	Computer Line
4.9 Hot Spot	New 4.9 Hot Spot		Actual Cost (Shipping & Material)	520250	Communication Equipment -Install
4.9 Access Point (New Location)	Cost of each new hot spot is unique. Circuit costs are the responsibility of the agency through the remainder of the fiscal year.		Actual cost including labor	520260	Computer Line
Consolette	Monthly maintenance charge for consolette	\$37.96 to \$217.83	Per Device per Month	520260	Computer Line
Radio Console	Console Monthly maintenance charge for dispatch console	\$62.54	Per Device per Month	520220	County Radio system
BDA	Monthly Maintenance charge for BDA	\$94.90	Per Month	520220	County Radio system
HPD	High Performance Data - Modem	\$108.05	Per Modem per Month	520260	Computer Line
Subscriber - portable	Monthly Charges for the base radio unit	\$37.96 to \$217.83	Per Network per Handheld	520220	County Radio system
Subscriber - repair	Material and shipping cost		Actual Cost (Shipping & Material)	521580	Maint-Radio Elec Equip
System Conventional	Monthly fee charged to users of a conventional radio system	\$334.03	Per Month	520220	County Radio System
Technologist Expert Time	Hourly shop and field radio repair rate	Per RCIT Approved Hourly Rate		521580	Maint-Radio Elec Equip
Technologist Expert Time - Premium	After hours (overtime) shop and field radio repair rate – Premium	Per RCIT Approved Premium Hourly Rate		521580	Maint-Radio Elec Equip

Microwave and Site					
Service Description	Definition	FY 12/13 Rate	Unit	Budget Account	Account Description
Rack Space (Full Rack)	Set rate for monthly rack mount charge	\$263.09	Monthly		
Rack RMU	Set rate for monthly rack mount per unit charge (partial rack)	\$65.77	Monthly		
Rack -Half Rack	Set rate for monthly rack unit charge(Half rack)	\$131.55	Monthly		
Floor Space (Excluding Rack Space)	Set rate for monthly square footage charge	\$320.83	Monthly		
Antenna Mounted Lower	Set rate for monthly LMR antenna lower	\$300.00	Position of the antenna per month		
Antenna Mounted Middle	Set rate for monthly LMR antenna middle	\$600.00	Position of the antenna per month	520280	Microwave
Antenna Mounted Top	Set rate for monthly LMR antenna top	\$900.00	Position of the antenna per month	520280	Microwave
Microwave Dish	Set rate for monthly microwave antenna	\$1,500.00	Per microwave antenna per month	520280	Microwave
Microwave Dish Weight	Additional rate for microwave dish weight	\$1.00	Per lb	520280	Microwave
T1	Monthly charge per T1 circuit mile	\$40.20	Per mile per month	520280	Microwave
Mile Analog	Monthly charge per analog circuit mile for microwave transmission	\$9.68	Per mile per month	520280	Microwave
DS3	Reserve for Fire Alessandro - North to Hemet	\$64.67	Per mile per month	520280	Microwave
Mile-56K	Monthly charges per 56K circuit mile for microwave transmission	\$16.08	Per mile per month	520280	Microwave

**Microwave and Site**

Service Description	Definition	FY 12/13 Rate	Unit	Budget Account	Account Description
PTP Wireless Connection	Monthly charge per connection for wireless WAN	\$46.13	Per connection per month	520280	Microwave
Un-licensed Wireless PTP	Monthly circuit charge for dedicated point-to-point WAN connection utilizing un-license wire point-to-point technology	\$493.79	Per circuit per month	520280	Microwave
Technologist Expert Time	Hourly Microwave and Site repair rate	Per RCIT Approved Hourly Rate		520280	Microwave
Technologist Expert Time - Premium	After hours (overtime) Microwave and Site repair rate – Premium	Per RCIT Approved Premium Hourly Rate		520280	Microwave
Tenant escort to the site during business hours	Tenants escort during business hours	\$74.92	Hourly	520280	Microwave
Tenant escort to the site after business hours	Tenants escort after business hours	\$112.38	Hourly	520280	Microwave

**Vehicle**

Service Description	Definition	FY 12/13 Rate	Unit	Budget Account	Account Description
Subscriber - Mobile	Monthly Charges for the base radio unit	\$37.96 to \$217.83	Per Network per Mobile	520220	County Radio System
Subscriber - Mobile repairs	Material and Shipping	Actual Cost (Shipping & Material)	Actual Cost (Shipping & Material)	521500	Maint-Motor Vehicle
MDC Data	Software Modification and repairs	\$28.71	Per unit	520220	County Radio system
Vehicle installation and repairs	Time and Material	Actual Cost (Shipping & Material)	Actual Cost (Shipping & Material)	521500	Maint-Motor Vehicle

**Technology Engineering**

Service Description	Definition	FY 12/13 Rate	Unit	Budget Account	Account Description
Data Engineering Expert Time	Hourly rate to design, implement and/or maintain Data communication networks and infrastructure of Countywide Communication facilities.	Per RCIT Approved Hourly Rate		524820	Engineering Services
Data Engineering Expert time – Premium	Weekend or after-hours rate to design, implement and/or maintain Data communication networks and infrastructure of Countywide Communication facilities	Per RCIT Approved Premium Hourly Rate		524820	Engineering Services
Infrastructure Engineering Expert Time	Hourly rate to design, implement and/or maintain Data communication networks and infrastructure of Countywide Communication facilities.	Per RCIT Approved Hourly Rate		524820	Engineering Services
Infrastructure Engineering Expert Time – Premium	Weekend or after-hours rate to design, implement and/or maintain Data communication networks and infrastructure of Countywide Communication facilities	Per RCIT Approved Premium Hourly Rate		524820	Engineering Services
Radio Engineering Expert Time	Hourly rate to design, implement and/or maintain Radio communication networks and infrastructure of Countywide Communication facilities.	Per RCIT Approved Hourly Rate		524820	Engineering Services
Radio Engineering Expert Time – Premium	Weekend or after-hours rate to design, implement and/or maintain Data communication networks and infrastructure of Countywide Communication facilities	Per RCIT Approved Premium Hourly Rate		524820	Engineering Services

**Pass Thru Account**

Service Description	Definition	FY 12/13 Rate	Unit	Budget Account	Account Description
Fire Network Infrastructure	Actual Cost	\$82,821.00	Actual Cost	520250	Communication Equipment - Install

**Rates for Non-County Agencies**

Rates for non-County Agencies will be negotiated individually with each department.

**Part-Time Usage Rate**

(The rate for part time users includes any agency that will use the system during pre-planned exercises, monthly verification testing, and during any County emergency)

The rate for part time users will be the lowest monthly subscriber rate.

# Exhibit C – Staffing Plan

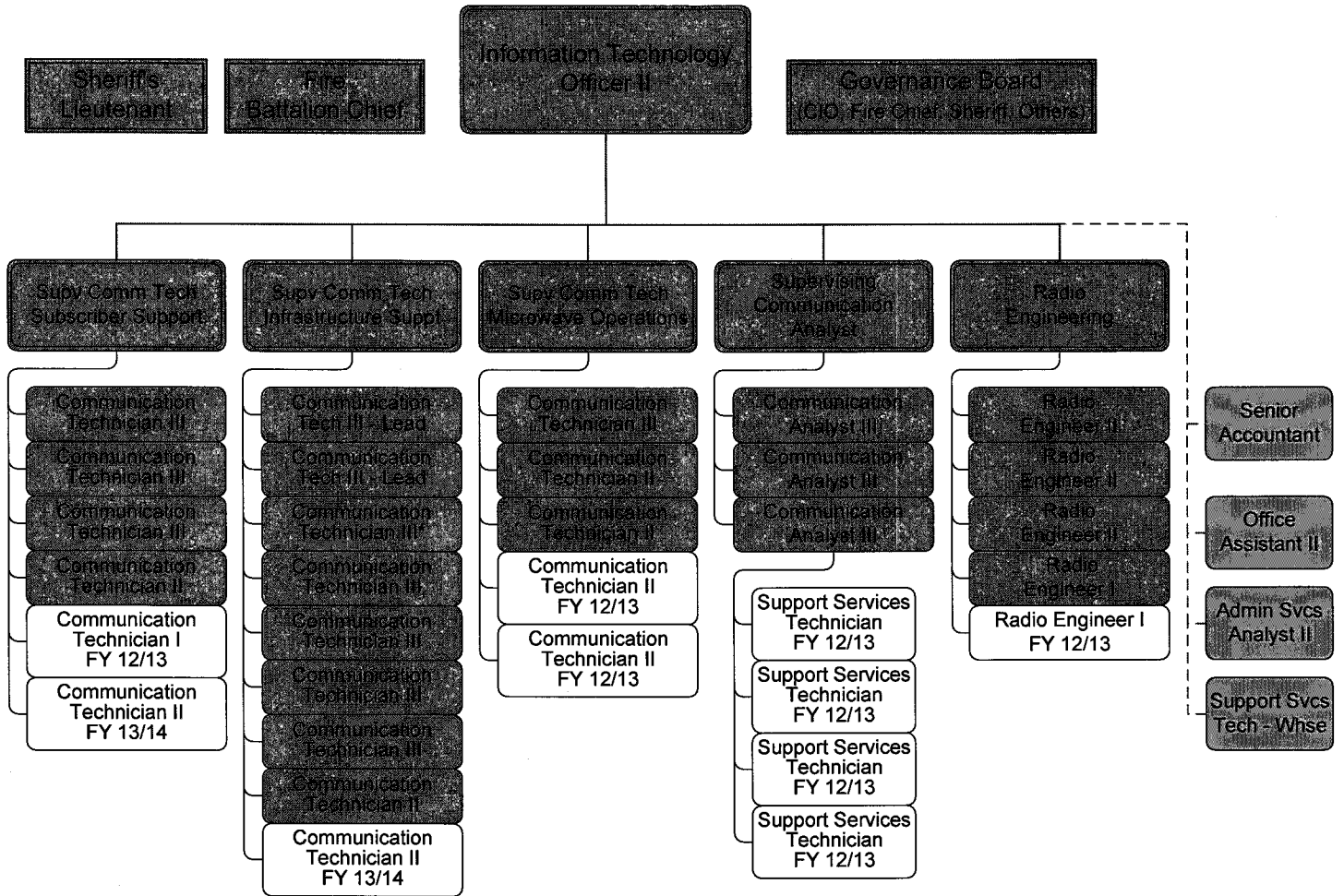
---

- One (1) Communications Solutions Senior Manager (Information Technology Officer II) to provide program management oversight including budgets, recruitment, process assessment and improvement, identify and address client's radio communication needs, services and ensuring quality control.
- One (1) Sheriff's Lieutenant to provide ongoing quality and commitment to Sheriff's Department concerns, needs, training, planning, organization, maintenance tracking and accounting of Sheriff related user equipment.
- One (1) Fire Battalion Chief to provide ongoing quality and commitment to County Fire's concerns, needs, training, planning, organization, maintenance tracking and accounting of Fire related user equipment.
- Two (2) Radio Communications Engineer I – under general supervision, to perform professional radio communications engineering work in connection with planning, design, construction, surveying or frequency licensing and or radio frequency interference; provides technical direction, instruction and/or training to field technicians; and to do other work as required.
- Three (3) Radio Communications Engineer II – perform varied and difficult professional radio communications engineering work which may involve planning, design, construction, surveying, or frequency licensing and/or radio frequency interference; provide technical direction, instruction and/or training to field technicians
- Three (3) IT Supervising Communication Technician – Supervise staff engaged in planning, organizing, constructing, adapting, installing, testing, maintaining and/or repairing communication equipment (data, voice, microwave, radio) and/or components of data, voice, radio, microwave and server based systems
- One (1) IT Supervising Communication Analyst – Supervise staff engaged in planning, organizing, constructing, adapting, installing, testing, maintaining and/or repair communication equipment (data, voice, microwave, radio) and/or components of data, voice, radio, microwave and server based systems
- Three (3) IT Communication Analyst III – Design, implement and/or maintain Communication networks (data, voice, video, image and radio)
- One (1) IT Communication Technician I – perform a variety of skilled and semi-skilled maintenance and repair work on a variety of desktop systems and peripherals (to be filled from RCIT Customer Services Division Staff)
- Eight (8) IT Communication Tech II – Plan, organize, construct, adapt, install, test, maintain and/or repair communication equipment (data, voice, microwave, radio) and/or components of data, voice, radio, and microwave
- Eleven (11) IT Communication Technician III – Plan, organize, construct, adapt, install, test, maintain and/or repair communication equipment (data, voice, microwave, radio) and/or components of data, voice, radio, microwave



- Four (4) Support Services Technician – perform skilled and semi-skilled repair and maintenance work; maintain record of repairs, minor maintenance projects, items received and issued; to assist in the installation mobile radio equipment; perform authorized repairs to communication/electronic equipment.
- RCIT Funded/Staffed Positions:
  - One (1) Office Assistant II – provide clerical support services (to be filled from RCIT Administrative Services staff.)
  - One (1) Senior Accountant – examine and analyze fiscal records, establish, review, revise, and maintain controls of the fiscal record keeping functions and assigned unit (to be filled from the RCIT Business Administration Services Staff)
  - One (1) Administrative Services Analyst II – assist management with a wide variety of administrative support; conduct complex and difficult research and analytical studies involving budgetary and/or operational processes and programs; make recommendations for the development, implementation, and improvement of departmental operations, services and programs and/or budgetary expenditure (to be filled from the RCIT Business Administration Services Staff)
  - One (1) Warehouse Technician – assist and support PSEC project with warehousing of PSEC materials (to be filled from the RCIT Business Administration Services Staff)

# PSEC Organization Chart



# Exhibit D– Governance Board Overview

---

## *Executive Summary*

The very nature of providing emergency services to the citizens of Riverside County requires reliable, robust interoperable communication. Responding to house fires, auto accidents and other emergency responses involves multi-disciplined agencies providing firefighting, emergency medical treatment and law enforcement services. These responses are most efficient and effective when these agencies can talk to one another using a single common radio network.

The success of a major project like public safety communication interoperability in Riverside County will require a process that includes communication, coordination, planning and on-going management. This process, and a key component of successful interoperability, is *Governance*.

Successful collaboration results from building bridges and fostering communications. By listening to each other, we can find commonalities, which serve to break down barriers between groups. Once a shared vision is developed, there must be a series of actionable steps to reaching the collaborative goals. Setting short-term, actionable goals that can be achieved incrementally and long term goals for governance of the System is a very important element. Interoperability requires the commitment of different agencies in the public safety community with responsibilities in a time of crisis. Leadership buy-in is a critical element of this. The PSEC Governance Board is the environment in which this collaboration will take place.

The National Governors Association Center for Best Practices in the issue brief “Achieving Statewide Public Safety Wireless Interoperability” stated:

“The governance structure is instrumental to building out an interoperable communications system. Not only does the governance structure solidify relationships and bring various stakeholders to the table, this body provides a vehicle for exploring innovative technologies and potential funding to achieve a given jurisdiction’s vision of interoperability.”

Including local representation on the governance body and in the interoperability planning process is critical. The state governance board that oversees the development of public safety communication needs to include the local public safety agency requirements for emergency communications.

Increasingly, across the country, governance bodies are using the title of **State Interoperability Executive Committee** (SIEC). For example, during 2003, the State of California, under the Office of Emergency Services, formed California Statewide Interoperability Executive Committee (CALSIEC). The term was used by the Federal Communications Commission in its order on 700 MHz spectrum planning. Whatever title is chosen, the concept of an oversight board requires much support from other entities.

The National Task Force on Interoperability in its report “Why Can’t We Talk” puts the proposition clearly that:

“The key to a successful effort resides within the strengths of committed leadership and the governance structure. Well-defined and structured governance will empower the effort because it requires the cooperation of both the public safety agencies and elected

and appointed officials. These groups possess the detailed process knowledge about their communities, regions and municipalities that can provide deep and broad perspectives on interoperability needs. Elected and appointed officials can play vital roles in the development, implementation and institutionalization of interoperability. Working together, they can give governance structures a voice in the political arena and statutory authority, help fund interoperability efforts, and bring professional management and knowledge to the process.”

There are a multitude of Public Safety Regional Communication Center governance processes in use today across the country at both the state and local levels. After researching the dominant models, PSEC has concluded that several characteristics permeate these structures:

- They are all a work in progress. Most have only been operating for a few years and are still in the stages of developing their charters and operating procedures. While some have made more progress than others have, they are still learning from their early experience and from each other.
- PSEC has identified the critical success factors from the most-successful efforts and has packaged them into a recommendation for Riverside County that builds upon the experiences of others but customizes it to the political and operational environment of the County and local stakeholders.
- There is a need for strong sponsorship, preferably at the highest levels to insure that the stakeholders see that this is a serious and committed effort on the part of everyone. Stipulation of clear goals and objectives, as well as limitations of power, are critical for the governance body and stakeholders to understand.

## *Introduction*

### *Mission Statement*

The mission of the PSEC Governance Board is to provide a collaborative environment for stakeholders of the PSEC Regional System to cooperatively make enterprise system, management and budgetary decisions and to improve public safety interoperability.

### *Purpose*

The purpose of the PSEC Governance Board is to improve communications and operations among participating public safety and service agencies. Approval of the Governance Board by the Riverside County Board of Supervisors establishes an organizational and management structure for ongoing network administration, operation, and maintenance. The Board will provide a process for admitting other public safety and public service entities to join and participate in the PSEC System and will collaboratively define the allocation of costs associated with the network’s operations, maintenance, and enhancement for members, both internal and external to Riverside County.

### *General Duties of Governance Board*

The Governance Board will set PSEC policy, prioritize projects, approve capital expenditures, approve the capital budget, and provide oversight and direction. The Governance Board may exercise such other powers and duties as authorized by the Riverside County Board of Supervisors.

### *Governance*

A governance structure for a regional system must be developed to ensure that participating agencies are provided with an environment of cooperation and cohesion. The PSEC System, although designed

with leading edge technology, will not effectively serve the public safety and public service agencies unless those agencies are involved in the decision making process for the System. A well-defined and structured governance board will empower the efforts behind the system because it requires the cooperation of the participating agencies.

To accomplish this, a governance board will be established to develop guidelines, create standard operating procedures and policies and enable agencies to work together toward a common goal and purpose.

One goal of the governance board will be to create equality among the agencies in major decisions affecting the PSEC system. This strategy could reduce or possibly eliminate the idea of one agency having control over another agency. The PSEC Governance Board will allow participating agencies, regardless of size, to have equal involvement and for their voice to be heard.

Another goal of the governance board is to increase chances for federal funding. The Department of Homeland Security's funding initiatives require regional systems, rather than single agency programs. The PSEC Governance Board and the participating agencies will make it possible for additional funding opportunities, to the benefit of all involved.

### *Models from Other Counties and States*

Counties and States that have successfully built, or are building countywide and statewide multi-jurisdictional public safety radio systems were researched on the question of governance. Some of the resulting organizations were formed through legislation, some were created by Executive Order, and still others were developed on an ad-hoc basis. Regardless of how they were created, they share a common mission of insuring that the public safety radio communication systems under their jurisdiction work well and are interoperable.

To accomplish this mission, oversight boards take similar paths, but have structures that reflect functions that are appropriate for the locale served. Some paths have been long in development but have yet to reach fruition. Conversations with State and County representatives, supplemented by information gathered by the NGA Center for Best Practices in Washington, DC, some examples of successful projects and the oversight structure employed are included in Attachment A.

### *Governance Structure*

The challenge for Riverside County is now to design a governance structure that reflects the Riverside County environment. The structure of the Governance Board will evolve as the Board refines the processes and procedures involved with the System. The foundational members of the Governance Board will be the current PSEC Steering Committee members or their designee

The first objectives of the Governance Board will be to determine:

- A Chairperson and Vice-Chairperson for the Board
- How Board membership is defined and managed
- How membership on the PSEC System is defined and managed
- The term and rotation pattern for positions on the Board
- The frequency of Board meetings
- The difference between regular, special and executive meetings
- How members will be added and removed from the Board, and what constitutes a need for removal from the Board

- How voting will be implemented and managed
- How a Quorum will be determined
- Approve policies and procedures for any activities that have a fiscal, operational, or administrative impact

# Exhibit E – Governance Board Policies

---



## Policies

Revised July 9, 2012

### Contents:

1. Proper Use of Network
2. Maintenance & Support
3. Change Control
4. Talkgroup Plan Approval
5. System Key Control
6. Password Administration
7. Access to Administrative Functionality
8. Remote Access
9. Recommended Form for Electronic Access Request

## *Proper Use of Network Policy*

Owner: <u>See Below</u>	Created: July 9, 2012	Category: Operations & Maintenance
Applicability: <u>See Below</u>	Revised: July 9, 2012	
Page: 1 of 2	Last Review: July 9, 2012	

### **1.0 Purpose**

- 1.1. The purpose of this policy is to define permissible communications and legitimate uses of the Public Safety Enterprise Communication (PSEC) network

### **2.0 Owner**

- 2.1. Communications Solutions Senior Manager

### **3.0 Applies To**

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

### **4.0 Background**

- 4.1. PSEC 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 PSEC network is required to ensure the system is available to support the intended purpose.

### **5.0 Policy Statement**

- 5.1. The PSEC network is authorized by the Federal Communications Commission to use frequencies allocated for public safety and public service operations. As such, use of the PSEC 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. Members are responsible for ensuring that appropriate training plans incorporate information on proper use of the PSEC network
- 7.2. 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 PSEC Governance Agreement.

**8.0 Conditions for Exemption of Waiver**

8.1. None

**9.0 Applicable Procedures**

9.1. Governance Agreement

9.2. Talkgroup Plan Approval Policy

9.3. Network Security (category) policies

<i>Maintenance &amp; Support Policy</i>		
Owner: <u>See Below</u>	Created: July 9, 2012	Category: Operations & Maintenance
Applicability: <u>See Below</u>	Revised: July 9, 2012	
Page: 1 of 6	Last Review: July 9, 2012	

## 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 PSEC in such a manner as to minimize the operational impact to participating agencies and their subscribers.
  - 1.1.1 Within which all maintenance activities pertaining to PSEC sites and facilities and PSEC infrastructure devices will be tracked and reported, including notification to Members of scheduled and unscheduled service affecting activities

## 2.0 Owner

- 2.1. Communications Solutions Senior Manager

## 3.0 Applies To

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

## 4.0 Background

- 4.1. The PSEC 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 Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the network.
- 4.2. The operational stability of PSEC may be affected when the configuration of the PSEC network is altered. Proper notification of scheduled and unscheduled service affecting maintenance activities will allow Members time to make necessary preparations. Conversely, unauthorized disruptions in PSEC operations caused by the lack of notification will create safety issues that must be addressed by the Communications Solutions Senior Manager.

## **5.0 Policy Statement**

- 5.1. The Communications Solutions Senior 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 PSEC are identified, triaged, and reported in such a fashion as to minimize the operational impact.
- 5.2. Members and other affected entities will be notified of any scheduled and unscheduled service affecting maintenance activities that have potential impact to the operational capabilities of the PSEC network or peripheral systems.
- 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 Communications Solutions Senior Manager.

## **6.0 Supporting Rules**

- 6.1. At least twenty-four (24) hours advance notice will be given to Members and other affected entities prior to service affecting maintenance activities
- 6.2. Service affecting maintenance activities not preceded by twenty-four (24) hour notice will be considered unscheduled maintenance
- 6.3. Notification of unscheduled service affecting maintenance will be made to the Members 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 Communications Solutions Senior Manager 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 and their designated alternates to be used for notification purposes will be kept in a central location and accessible from the Communications Solutions Senior 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 Communications Solutions Senior Manager.

- 6.9. All components of PSEC managed by the Communications Solutions Senior 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. Configuration files and event logs will be backed up as determined by the Communications Solutions Senior Manager.

## **7.0 Responsibilities**

- 7.1. The management of the PSEC infrastructure is the responsibility of the Communications Solutions Senior Manager
- 7.2. The Communications Solutions Senior Manager will establish on-call after-hour support for anomaly resolution
- 7.3. The Communications Solutions Senior Manager will ensure that PSEC reporting activities for anomalies will be conducted seven (7) days a week and twenty-four (24) hours a day
- 7.4. The Communications Solutions Senior Manager will:
  - 7.4.1. Establish and maintain processes and procedures for operations and maintenance of the PSEC 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 PSEC Members.
  - 7.4.8. Maintain current software licensing on all PSEC infrastructure components.
  - 7.4.9. Maintain technical support necessary to operate, troubleshoot, and optimize the PSEC infrastructure.

- 7.4.10. Incident types, response times, and appropriate actions are defined by severity level in accordance with procedures established by the Communications Solutions Senior 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 PSEC infrastructure in a manner that is consistent with industry best practices and manufacturer recommendations.
- 7.4.13. Operate the PSEC network in accordance with the Network Security category policies.
- 7.4.14. Responsible for notifying the Members of scheduled and unscheduled service affecting maintenance activities.
- 7.5. PSEC Alessandro is the point of contact for key management and encryption. Requests for key management and encryption support are to be submitted to the team during normal business hours if possible. After hours, the point of contact for emergency support of key management and encryption is the on call Radio Operations Supervisor.
- 7.6. Members are responsible for providing their own dispatch console maintenance
  - 7.6.1. Members are responsible for notifying the Communications Solutions Senior Manager of maintenance activities on their consoles.
- 7.7. Members are responsible for communicating scheduled and unscheduled PSEC maintenance activities to their respective agencies and, if necessary, their respective dispatch centers
- 7.8. Members are responsible for notifying Communications Solutions Senior 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

<i>Change Control Policy</i>		
Owner: <u>See Below</u>	Created: July 9, 2012	<b>Category: Configuration Management</b>
Applicability: <u>See Below</u>	Revised: July 9, 2012	
Page: 1 of 4	Last Review: July 9, 2012	

## 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 PSEC 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. Communications Solutions Senior Manager

## 3.0 Applies To

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

## 4.0 Background

- 4.1. Each component of the PSEC network infrastructure has a desired configuration that controls the operational capabilities of PSEC. Changes to the infrastructure configurations will be required from time to time. Because changes to the 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 PSEC network infrastructure configurations are properly requested, analyzed, tested, approved, documented and implemented.
- 5.2. No service affecting modifications will be made to any PSEC infrastructure configurations without the review and approval of the Communications Solutions Senior Manager and in accordance with the "Maintenance & Support Policy."

## 6.0 Supporting Rules

- 6.1. The Communications Solutions Senior Manager will coordinate all PSEC network infrastructure configuration changes.

- 6.2. All requests for network infrastructure configuration changes will be evaluated by the Communications Solutions Senior Manager for potential operational impact to subscriber agencies.
- 6.3. All network infrastructure parameter change requests will be reviewed by committees established by the Executive Director.
- 6.4. Each service affecting change to an infrastructure configuration will be thoroughly tested by the Communications Solutions Senior Manager.
- 6.5. 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.

## **7.0 Responsibilities**

- 7.1. The Communications Solutions Senior 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.
- 7.2. The committees established by the Executive Director will be responsible for reviewing proposed changes to the PSEC network infrastructure parameter(s), assessing the impact of the change request, and providing feedback (recommendation) to Communications Solutions Senior Manager relative to the change request.
- 7.3. The Communications Solutions Senior 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.
- 7.4. The Communications Solutions Senior Manager will be responsible for collecting and retaining all documentation relative to the infrastructure change.

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

- 8.1. Routine activities that result in changes to PSEC network infrastructure components such as adding subscribers to the UCS or other routine activities as determined by the Communications Solutions Senior Manager will be exempt from this policy.
- 8.2. During catastrophic events or emergency situations, immediate changes to the PSEC network infrastructure are authorized based on the judgment of the Communications Solutions Senior Manager, in consideration of all PSEC users, with Public safety considerations having the highest priority. The Communications Solutions Senior Manager will immediately notify the Executive Director, Members, and Area Managers, as time allows.

**9.0 Applicable Procedures**

- 9.1. Recommended form for Requests for Changes (following page of this policy)
- 9.2. 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</b> (Task Definitions, Schedule, Responsibility, Recovery Strategy)	
<b>Communications Solutions Senior Manager Recommendation</b>	
<b>Feedback (Recommendation) From The Committees Established By The Executive Director</b>	
<b>Additional Comments</b>	



# *Talkgroup Plan Approval Policy*

Owner: <u>See Below</u>	Created: July 9, 2012	Category: Configuration Management
Applicability: <u>See Below</u>	Revised: July 9, 2012	
Page: 1 of 6	Last Review: July 9, 2012	

## **1.0 Purpose**

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

## **2.0 Owner**

2.1. Communications Solutions Senior Manager

## **3.0 Applies To**

3.1. Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the PSEC 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 PSEC system performance, the Communications Solutions Senior Manager will review and approve all talkgroup plans and proposed changes.

## **6.0 Supporting Rules**

6.1. Each 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 PSEC will develop a preliminary talkgroup plan that considers internal business operations and any requirements for communications with other PSEC entities.

6.4. Upon completion of the preliminary talkgroup plan, the agency shall submit the preliminary plan to the Communications Solutions Senior Manager for technical and operational analysis.

- 6.5. The Communications Solutions Senior 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 Communications Solutions Senior 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

## *System Key Control Policy*

Owner: <u>See Below</u>	Created: July 9, 2012	Category: Network Security
Applicability: <u>See Below</u>	Revised: July 9, 2012	
Page: 1 of 4	Last Review: July 9, 2012	

### **1.0 Purpose**

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

### **2.0 Owner**

- 2.1. Communications Solutions Senior Manager

### **3.0 Applies To**

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

### **4.0 Background**

- 4.1. PSEC 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 PSEC 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 r anomalies to subscriber operations.
- 4.2. The System Key may take the form of a "software" System Key or an "Advanced" System Key ("ASK"). The ASK is comprised of two components, a "parent" key and "child" key(s). There is only one parent key per system, but there may be multiple child keys per system.
- 4.3. The System Key must be programmed into any subscriber unit that operates directly on PSEC. These subscriber units include all Members, Associates, Interoperability Participants, and Conditional Participants, and could also include radio units from other entities that are given access rights to use PSEC.
- 4.4. PSEC public safety departments have operational requirements and mutual aid agreements that require they interoperate with non-PSEC entities. Direct interoperability (automatic unit to unit) is supported by programming non-PSEC subscriber equipment with the PSEC System Key.
- 4.5. 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 PSEC subscriber programming equipment shall at all times employ appropriate operational and network security practices, as adopted by the Communications Solutions Senior Manager, to protect PSEC users from programming errors that could potentially cause disruptions or failures in service.
- 5.2. The Communications Solutions Senior Manager will control the PSEC System Key. The PSEC software System Key and the ASK parent key will not be released to Members, Associates, Interoperability Participants, Conditional Participants, or their Contractors.
- 5.3. An ASK child key will be released to Members, Associates, Interoperability Participants, or Conditional Participants in accordance with the provisions described herein.
  - 5.3.1. A separate ASK child key and request form will be required for each programming template to be used with the ASK child key (i.e. law enforcement, fire, public works).

## **6.0 Supporting Rules**

- 6.1. The Communications Solutions Senior Manager will provide all routine and emergency PSEC radio programming services for the Members, Associates, Interoperability Participants, and Conditional Participants as defined in the PSEC Governance Agreement.
- 6.2. Requests for programming of the PSEC System Key into non-PSEC radios shall be made by the appropriate representative of the requesting agency to the PSEC Governance Board Chair.
- 6.3. The Communications Solutions Senior Manager will provide, upon approval by the PSEC Governance Board Chair, programming services for authorized non-PSEC radios for interoperable service as defined in the PSEC Governance Agreement.
- 6.4. Any breaches in PSEC System Key use shall immediately be reported to the Communications Solutions Senior Manager and PSEC Governance Board Chair who shall take immediate steps to minimize the danger to the operational capabilities of PSEC.
- 6.5. An ASK child key will be issued upon acceptance of a written request by a Representative to the PSEC Governance Board Chair containing the information on the "Advanced System Key (ASK) Child Key Request" form.
- 6.6. The following rules apply to the issuance of an ASK child key:
  - 6.6.1. Adherence to this Policy, in particular the need to safeguard the ASK child key and report the loss of an ASK child key as required in section 6.4.

- 6.6.2. Agreement to pay the hardware cost of the ASK child key and for the Communications Solutions Senior Manager's time to create the ASK child key and associated template development.
  - 6.6.2.1. A time & material "Two-Way Radio Equipment Maintenance Agreement" with the County of Riverside is required to enable billing of the costs above (not a monthly recurring fee).
- 6.6.3. Timely notification to the Communications Solutions Senior Manager if a radio programmed with their ASK child key is missing, lost, stolen, destroyed, or otherwise rendered inoperable.
- 6.7. Upon notification by the PSEC Governance Board Chair that a written request for an ASK child key has been accepted, the Communications Solutions Senior Manager will create an ASK child key and arrange for receipted transfer to the responsible party.
  - 6.7.1. The Communications Solutions Senior Manager will create an ASK child key specifying the radio identification number (ID) range and set the permissions (such as talkgroups, functions, templates) for the requestor to program radios on the PSEC network.
  - 6.7.2. The Communications Solutions Senior Manager will work with the responsible party to develop a radio programming template for use with the ASK child key being issued.
  - 6.7.3. The ASK child key will be set to expire 18 months after the date the ASK child key is created. An expired ASK child key must be replaced, by initiating the process described in section 6.5, above.
  - 6.7.4. The ASK child key will be issued with password protection enabled. The password will be communicated to the responsible party.
  - 6.7.5. The responsible party is required to notify the Communications Solutions Senior Manager of the radio identification number(s) (ID) and radio serial numbers to be enabled in the infrastructure before the radio will be operational on the PSEC network.
- 6.8. PSEC reserves the right to audit the ASK child key, radio identification numbers (IDs), and associated templates.

## **7.0 Responsibilities**

- 7.1. The Communications Solutions Senior Manager is responsible for the development of internal controls for protection of the PSEC System Key.
- 7.2. The Communications Solutions Senior 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 Communications Solutions Senior Manager and PSEC Governance Board Chair for resolution.

**8.0 Conditions for Exemption or Waiver**

8.1. None

**9.0 Applicable Procedures**

9.1. PSEC Governance Agreement

9.2. Recommended Form for Advanced System Key (ASK) Child Key Request

9.3. County of Riverside Two-Way Radio Equipment Maintenance Agreement

*Advanced System Key(ASK) Child Key Request Form*

Owner: <b><u>See Below</u></b>	Created: <b>July 9, 2012</b>	<b>Category: Network Security</b>
Applicability: <b><u>See Below</u></b>	Revised: <b>July 9, 2012</b>	
Page: <b>1 of 1</b>	Last Review: <b>July 9, 2012</b>	

**To be completed by Advanced System Key (ASK) Child Key Requester**

(all lines below are required to be filled in)

Organization	
Representative Name	
Date of Request	

**Responsible Party Information**

Name	
Job Title	
Mailing Address	
City, State, Zip	
Telephone Number	
Email Address	
Representative acknowledges receipt of the attached PSEC System Key Control Policy	
Signature of Representative	

**To be completed by the PSEC Executive Director**

Signature & Date for acceptance of ASK Child Key Request

**To be completed by Communications Solutions Senior Manager**

ASK Child Key Created Date and Expiration Date			
Date Created		Expiration Date	

# *Password Administration Policy*

Owner: <u>See Below</u>	Created: July 9, 2012	Category: Network Security
Applicability: <u>See Below</u>	Revised: July 9, 2012	
Page: 1 of 3	Last Review: July 9, 2012	

## **1.0 Purpose**

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

## **2.0 Owner**

- 2.1. Communications Solutions Senior 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 PSEC 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 Communications Solutions Senior Manager will establish and maintain the necessary processes and procedures to ensure that passwords to include the read, write, and executable functions of the PSEC 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. PSEC passwords should contain both upper and lower case letters when applicable.
- 6.4. PSEC passwords should have numbers (0-9) and letters.
- 6.5. PSEC passwords must be at least eight characters in length.



- 6.6. PSEC 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. PSEC users must not create passwords that are identical or substantially similar to passwords they previously employed.
- 6.10. PSEC passwords should never be written down or stored on-line.
- 6.11. PSEC users must not use the same password for PSEC accounts as for other non-PSEC access.
- 6.12. PSEC users must not use the "Remember Password" feature of any PSEC 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 Communications Solutions Senior Manager immediately.

## **7.0 Responsibilities**

- 7.1. The Communications Solutions Senior 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 Communications Solutions Senior Manager will conduct a password audit and provide the PSEC Governance Board Chair, 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 Communications Solutions Senior Manager will ensure that all PSEC personnel are aware of the Password Administration Policies.
- 7.4. The Communications Solutions Senior 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 PSEC Governance Board Chair.

- 7.5. The Communications Solutions Senior Manager will maintain all electronic access request records.
- 7.6. The Communications Solutions Senior 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 PSEC will acknowledge the receipt, comprehension and adherence of the PSEC Password Administration Policies by signature, which will be returned to the Communications Solutions Senior Manager.

**8.0 Conditions for Exemption or Waiver**

- 8.1. In the event an emergency, the Communications Solutions Senior 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

# *Access to Administrative Functionality Policy*

Owner: <u>See Below</u>	Created: July 9, 2012	Category: Network Security
Applicability: <u>See Below</u>	Revised: July 9, 2012	
Page: 1 of 3	Last Review: July 9, 2012	

## **1.0 Purpose**

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

## **2.0 Owner**

- 2.1. Communications Solutions Senior Manager

## **3.0 Applies to**

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

## **4.0 Background**

- 4.1. There are multiple software tools available in the PSEC 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 PSEC system administrative tools is restricted to users authorized by the Communications Solutions Senior Manager.

## **6.0 Supporting Rules**

- 6.1. Personnel with electronic access to the administrative functions of PSEC are required to have a current, signed recommended form for Electronic Access Request on file with the Communications Solutions Senior Manager.. These documents may be subject to renewal at regular intervals.
- 6.2. The Communications Solutions Senior 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 Communications Solutions Senior Manager immediately.

## **7.0 Responsibilities**

- 7.1. The Communications Solutions Senior 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

## *Remote Access Policy*

Owner: <u>See Below</u>	Created: July 9, 2012	Category: Network Security
Applicability: <u>See Below</u>	Revised: July 9, 2012	
Page: 1 of 3	Last Review: July 9, 2012	

### **1.0 Purpose**

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

### **2.0 Owner**

- 2.1. Communications Solutions Senior Manager

### **3.0 Applies To**

- 3.1. Members, Associates, Interoperability Participants, and Conditional Participants that have operational subscribers on the network, and all contractors.
- 3.2. This policy covers all PSEC 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 PSEC 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 PSEC is prohibited unless expressly permitted by the Communications Solutions Senior Manager.

### **6.0 Supporting Rules**

- 6.1. All 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 Communications Solutions Senior Manager, in advance, their requests for remote access to PSEC 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 Communications Solutions Senior 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 PSEC.
- 6.4. Any computer permitted remote access to the PSEC network requires certification to the Communications Solutions Senior 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 PSEC 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 Communications Solutions Senior Manager whenever any user who has been granted remote access no longer requires access to the PSEC network or PSEC related equipment.
- 6.7. Any computer with the ability to access PSEC and other non-PSEC 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 PSEC 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 Communications Solutions Senior Manager will establish and maintain the necessary processes and procedures to prohibit, unless expressly permitted, remote access to PSEC 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 Communications Solutions Senior Manager will ensure that a centralized user access control list will be maintained to determine, audit and report who is authorized to remotely access PSEC.
- 7.3. The Communications Solutions Senior 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 Communications Solutions Senior Manager will notify the Executive Director of any remote access attempts deemed of a suspicious or malicious nature.

- 7.5. The Communications Solutions Senior Manager will ensure that any changes to firewall configurations and/or access control lists will be reviewed and approved.
- 7.6. The Communications Solutions Senior 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: <b>See Below</b>	Created: <b>July 9, 2012</b>	<b>Category: Network Security</b>
Applicability: <b>See Below</b>	Revised: <b>July 9, 2012</b>	
Page: 1 of 1	Last Review: <b>July 9, 2012</b>	

**To be completed by Electronic Access Requester**

Name	
Agency / Department	
Date	
Functionality Requested	
Reason For Request	
Duration Required	
Request for Access and Acknowledgement of PSEC Password Administration Policy	
Signature	

**To be completed by Communications Solutions Senior Manager**

Access Granted Date	
---------------------	--



# ATTACHMENT B

## Policy B-26

County of Riverside, California  
Board of Supervisors Policy

Subject:  
**LEASING OF COUNTY-OWNED REAL PROPERTY  
FOR WIRELESS SERVICE FACILITIES**

<u>Policy Number</u>	<u>Page</u>
<b>B-26</b>	<b>1 of 2</b>

### Policy:

Board Policy B-26 specifies procedures for leasing County-owned sites for wireless communications and outlines procedures for the creation of site licenses, leases, subleases, lease amendments, lease renewals and other relevant documents for the use of real property owned by the county for allowable and appropriate uses by personal wireless communication service facilities providers. The policy outlines procedures to protect County owned and/or operated wireless communications and establishes guidelines for the use of fees and revenues from these locations.

### **PROCEDURES TO PROVIDE FOR THE USE OF COUNTY-OWNED REAL PROPERTY FOR THE PURPOSE OF WIRELESS SERVICE FACILITY LEASES**

#### **A. New Leases on County-Owned Real Property**

It is the policy of the County of Riverside to allow the use of County-owned lands and buildings by wireless communications providers. Such use improves routine communications services for the County's residents and the traveling public, improves public safety communications during emergencies, and provides incidental income to the County.

The Department of Facilities Management shall serve as lead agency for wireless service facilities on all County land and buildings and will negotiate terms and conditions of all licenses, leases, subleases, lease renewals, and lease amendments. No other County agency may negotiate such leases, and all County agencies are to immediately refer all wireless services inquiries to Facilities Management. Facilities Management will also negotiate and manage agreements to allow for co-location wireless communications at county public safety radio communications system sites.

Facilities Management is to work with the agency using the land to ensure that the proposed wireless facility will not unreasonably compromise the agency's use of the site. Facilities Management may recover its costs through an initial application fee and through its standard surcharge for lease administration. Prior to entering into the lease, Facilities Management shall submit the application to Riverside County Information Technology (RCIT), which shall in turn review the proposed installation to ensure that it will not interfere with the County's public safety radio system.

Subject:  
**LEASING OF COUNTY-OWNED REAL PROPERTY  
FOR WIRELESS SERVICE FACILITIES**

Facilities Management shall act as the permit authority and perform all plan check and construction inspection services, and shall ensure compatibility with existing building components and future County use of the real property.

Facilities Management is authorized to offer wireless communications lease management to County affiliated special districts, community facilities districts, joint powers agencies and authorities, and similar organizations. Facilities Management may employ consultants as needed to assist in the administration of wireless communications leases.

RCIT shall be authorized and directed to act on behalf of the County to perform technical review of all wireless services applications for proposed wireless service facilities on County-owned real property. RCIT shall ensure that there will be no interference with the county's public safety radio system as a result of the installation before Facilities Management enters into the lease and issues permits. RCIT may recover its costs through an initial application fee.

All existing leases between wireless service providers and County departments, agencies, and special districts shall comply with this policy upon renewal of the lease.

**B. Revenues**

Some County lands were purchased with funds which require lease or sale income to be returned to the purpose supporting the original funding. Facilities Management shall work with the appropriate County agency in determining if land income restrictions exist. Restricted lease revenues (such as revenue generated from Redevelopment Agency property, Parks and Open Space District and Flood Control District property, and restricted Transportation Department property) shall continue to be deposited into the respective entity's restricted funds. All other unrestricted revenue generated on County-owned property from wireless service facility leases and licenses shall be deposited into the RCIT public safety communications account and used to support the County's public safety communications system. An annual report on lease revenues generated under this program shall be prepared by Facilities Management and included in the department's mid-year budget report.

**Reference:**  
Minute Order 3.22 of 10/17/06  
Minute Order 3.3 of 04/10/07

**ATTACHMENT C**  
**RCIT – Communication Solution Division Fund**

Increase Appropriations:

45520 - 7400600000 – 510040 Regular Salaries	\$	1,662,641.00
45520 - 7400600000 – 510420 Overtime	\$	90,000.00
45520 - 7400600000 – 510500 Standby Pay	\$	75,000.00
45520 – 7400600000 – 517000 Workers Comp Insurance	\$	1,072.00
45520 - 7400600000 – 518100 Budgeted Benefits	\$	484,355.00
45520 - 7400600000 – 520220 County Radio System	\$	805,353.00
45520 - 7400600000 – 520230 Cellular Phone	\$	18,667.00
45520 - 7400600000 – 520260 Computer Lines	\$	494,253.00
45520 - 7400600000 – 520815 Cleaning and Custodial Supp	\$	485.00
45520 - 7400600000 – 521340 Maint-Communications Equipment	\$	43,710.00
45520 - 7400600000 – 521360 Maint-Computer Equipment	\$	9,450.00
45520 - 7400600000 – 521380 Maint-Copier Machines	\$	1,500.00
45520 - 7400600000 – 521460 Maint-Microwave Equipment	\$	107,000.00
45520 - 7400600000 – 521580 Maint-Radio Elec Equipment	\$	22,705.00
45520 - 7400600000 – 521640 Maint-Software	\$	27,718.00
45520 - 7400600000 – 522310 Maint-Building and Improvement	\$	616,367.00
45520 - 7400600000 – 523100 Memberships	\$	2,475.00
45520 - 7400600000 – 523220 Licenses and Permits	\$	17,975.00
45520 - 7400600000 – 523640 Computer Equipment-Non Fixed Asset	\$	12,100.00
45520 - 7400600000 – 523660 Computer Supplies	\$	5,000.00
45520 - 7400600000 – 523700 Office Supplies	\$	2,500.00
45520 - 7400600000 – 523760 Postage - Mailing	\$	2,500.00
45520 - 7400600000 – 523840 Computer Equipment-Software	\$	3,500.00
45520 - 7400600000 – 524740 County Support Service	\$	95,000.00
45520 - 7400600000 – 525020 Legal Services	\$	15,000.00
45520 - 7400600000 – 525440 Professional Services	\$	312,323.00
45520 - 7400600000 – 525440 Professional Services (contingency)	\$	110,796.00
45520 - 7400600000 – 526710 Rent-Lease Land	\$	568,708.00
45520 - 7400600000 – 526960 Small Tools and Instruments	\$	4,000.00

45520 - 7400600000 – 527100 Fuel	\$	980,018.00
45520 - 7400600000 – 527840 Training –Education/Tuition	\$	6,000.00
45520 - 7400600000 – 527880 Training –Other	\$	4,620.00
45520 - 7400600000 – 528920 Car Pool Expense	\$	208,367.00
45520 - 7400600000 – 528960 Lodging	\$	1,000.00
45520 - 7400600000 – 528980 Meals	\$	375.00
45520 - 7400600000 – 529540 Utilities	\$	425,000.00
45520 - 7400600000 – 532600 Cap Lease-Purch Principal	\$	1,306,853.00
45520 - 7400600000 – 533720 Cap-Lease Purchase Interest	\$	533,836.00
45520 - 7400600000 – 546060 Equipment –Communications	\$	175,000.00

Increase Estimated Revenue:

45520 - 7400600000 – 770790 700 MHz System	\$	6,066,172.00
45520 - 7400600000 – 770810 Replacement Radios	\$	1,618,727.00
45520 - 7400600000 – 770920 Microwave	\$	482,809.00
45520 - 7400600000 – 770930 R & E Equipment	\$	41,310.00
45520 - 7400600000 – 770940 R & E Labor	\$	444,937.00
45520 - 7400600000 – 770980 Vault Space	\$	599,267.00