

# Public Safety Radio

## Strategic Planning Committee:

*2007 Statewide Integrated Public Safety*

*Communications Strategic Plan*

---

*A plan for California State public safety communications system  
integration, modernization, and interoperability*

### **COMPENDIUM OF REFERENCES**

**TO REPORT TO THE CALIFORNIA STATE LEGISLATURE**

*as required by Government Code § 8592.6*

*January 1, 2007*

**Governor**  
**Arnold Schwarzenegger**

**PSRSPC Chair**  
**Henry R. Renteria**  
**Director, Governor's Office of Emergency Services**

## **COMPENDIUM OF REFERENCES**

<b>Appendix 1 - 2006 Online Assessment Survey</b>	<b>1</b>
<b>Appendix 2 - Requirements Definition</b>	<b>1</b>
<b>Appendix 3 - Evolving Systems Engineering Management Plan Considerations</b>	<b>7</b>
<b>Appendix 4 - FCC Licensing Issues Relative to the Use of Gateway Devices</b>	<b>10</b>
<b>Appendix 5- PSRSPC Statute as of January 1, 2007</b>	<b>16</b>
<b>Appendix 6 - Public Safety Radio Strategic Planning Committee resolution regarding compliance with TIA-102/APCO Project 25 standards (September 22, 2006)</b>	<b>20</b>

# Appendix 1 - 2006 Online Assessment Survey

(This section will contain survey questions only.)

## Appendix 2 - Requirements Definition

### Requirements Definition Goals & Objectives:

The evolving Statement of Requirements (SoR) must necessarily represent a comprehensive integrated public safety solution able to accommodate (to the greatest extent practicable) legacy, current, and future public safety wireless voice and data communications systems of those local, state, and federal government users having the wherewithal, willingness and legitimacy to participate.

Remain ever cognizant of the SAFECOM Program mantra that states, "...to drive progress along the five elements of the continuum and improve interoperability, public safety practitioners should observe the following principles:

- Gain leadership commitment from all disciplines [Emergency Medical Services (EMS), Fire, Law Enforcement],
- Foster collaboration across disciplines (EMS, Fire, Law Enforcement) through leadership support,
- Interface with policy makers to gain leadership commitment and resource support,
- Use interoperability solutions on a regular basis,
- Plan and budget for ongoing updates to systems, procedures, and documentation, and
- Ensure collaboration and coordination across all elements [Governance, Standard Operating Procedures (SOPs), Technology, Training/Exercises, Usage]."

To develop a System-of-Systems (SoS) based Statement of Requirements (SoR):

- Focused on the functional needs of public safety first responders—Emergency Medical Services (EMS) personnel, firefighters, and law enforcement officers—to communicate and share information as authorized when it is needed, where it is needed, and in a mode or form that allows the practitioners to effectively use it. The communications mode may be voice, data, image, video, or multimedia that includes multiple forms of information.
- Rooted in the goal of improving the ability of public safety personnel to communicate among themselves, with the non-public safety agencies and organizations with whom they work, and with the public that they serve

To assist the telecommunication interoperability and information-sharing efforts by and among local, tribal, state, and federal government agencies, and regional entities, by delineating the critical operational functions and interfaces within public safety communications that would benefit from research and development investment and standardization.

**Key Elements/Issues to be expanded upon:**

- **Public Safety Requirements and Roles**, defines public safety communication needs and public safety roles and functions.
- **Communications Services Definition** defines communications services—interactive and non-interactive voice communications and interactive and non-interactive data communications.
- **Public Safety Wireless Communications Scenarios** outlines several public safety scenarios based on typical operations to provide a view of future public safety communications.
- **Operational Requirements of Public Safety for Wireless Communications and Information Capabilities** identifies the wireless communications operational needs of public safety.
- **Wireless Communications Functional Requirements** defines the wireless communications functional requirements.
- **Complete Glossary** of the terminology and acronyms used in the SoS-oriented SoR.
- **System Capabilities** including:
  - **Wireless Voice Capabilities**
    1. **Communications Regardless of Technologies, Infrastructures, and Frequency Bands**

Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions some of which may use different technologies, infrastructures and/or frequency bands regardless of system. Includes the transitioning between commercial systems and private LMR systems.
    2. **Communication with Own Jurisdiction**

Ability to communicate with members of own agency/jurisdiction while using the infrastructure of another agency/jurisdiction.
    3. **Communication with Other Jurisdictions**

Ability to communicate with other agencies/jurisdictions using the infrastructure of that agency/jurisdiction.

4. **One-to-One Communications**  
Ability for users to transparently communicate, as authorized, with members of other agencies/jurisdictions on a unit-to-unit (one-to-one) basis.
5. **One-to-Many Communications**  
Ability for users to transparently communicate, as authorized, with members of other agencies/jurisdictions on a unit-to-group (one-to-many) basis.
6. **Communications Outside Wireless Infrastructure Coverage**  
Provide direct communications (talk around) between user radios where wireless infrastructure is unable to support communications (such in some rural areas, underground parking garages, tunnels, and inside some buildings).
7. **Jurisdictional Signal Coverage**  
Provide jurisdictional-wide signal coverage to system users; optionally, provide ways to enhance or improve jurisdictional coverage into rural areas, underground parking garages, tunnels, and inside buildings that are usually not sufficiently covered.
8. **Identification and Authorization**  
Ability to initiate wireless voice communications by requiring the user to enter (on his/her radio) a user identification that authenticates and validates the user and loads the user's profile. This profile defines talk groups for the user and completes all radio network administration for the user's voice communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.
9. **Priority Levels for Access and System Use**  
Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular public safety applications (such as task force operations, incidents, etc.).
10. **Emergency Voice Communication**  
Ability to communicate an emergency voice message (e.g. after pressing a panic button) that has priority over other voice communications.
11. **Emergency Signal**  
Ability to broadcast an emergency signal (e.g. via a panic button) that has priority over other communications.
12. **Secure Communications**

Ability to have secure (encrypted) voice communications to fit users' environment and which satisfies applicable laws, regulations, policies of the agencies and jurisdictions of the users.

13. System Administration

Ability to effectively initiate and sustain flexible and dynamic system administration for purposes of multi-agency interoperability, including administration of talk groups, encryption key management, emergency alerts, networks, and channels for mutual aid.

14. Remotely Re-Program User Radios

Ability to remotely (over-the-air) re-program a radio's parameters (i.e., frequency channels, talk groups, squelch control, encryption keys, etc.) and/or modify functionality (e.g., encryption algorithms, waveforms, etc.)

15. Resilient Operations

Ability to sustain resilient operations including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc.

16. Reliable System Performance

Ability to maintain reliable system performance over disparate interconnected systems.

• **Wireless Data Capabilities**

17. On-scene Wireless Data Networks

Ability to quickly and transparently establish and maintain on-scene wireless data networks (e.g., on-scene to include in-building).

18. On-scene Exchange of Data

Ability of on-scene personnel to transparently exchange data.

19. High-Speed Data Transfer

Capability of high-speed data transfer with ability to sustain performance at network interconnections.

20. Communication with Own Jurisdiction

Ability to exchange data with members of own agency/jurisdiction while using the infrastructure of another agency/jurisdiction.

21. Communication with Other Jurisdictions

Ability to exchange data with members of other agencies/jurisdictions using the infrastructure of that agency/jurisdiction.

22. Sensor Networks

Ability to exchange data involving sensors (e.g., biometric, environmental, personnel location).

23. Identification and Authorization

Ability to initiate wireless data communications by requiring the user to enter (on his/her terminal/radio) a user identification that authenticates and validates the user and loads the user's profile. This profile defines data resource capabilities for the user and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as previously authorized.

24. System Administration

Flexible and dynamic system administration (includes administration of wireless data networks, adding users, giving permissions).

25. Data Security

Ability to ensure secure exchange of information.

26. Information Protection

Ability to protect information according to applicable laws and statutes.

27. Resilient Operations

Ability to sustain resilient operations including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc.

28. Reliable System Performance

Ability to maintain reliable system performance over disparate interconnected systems.

• **Information Systems Capabilities**

29. Rapid Information Source Access

Ability to provide the exchange of information in a timely fashion to support critical decision points from both field and base locations, including but not limited to information regarding identification (photos, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, CAD info, building diagrams, building sensors, transportation info, etc.).

30. Query/Access Multiple Data Sources with One Request

Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.

31. "Enter Once – Reuse Forever" Approach to Data Gathering

Ability to enter validated information once, then share and reuse that information among authorized entities.

32. Data Exchange with Computer-Aided Dispatch

Ability to exchange information with Computer-Aided Dispatch (CAD) and Record Management Systems (RMS).

33. Data Access to Logistical Resource Information  
Capability to obtain logistical resource information on all personnel and equipment responding to an incident.
34. Emergency Notifications  
Ability to broadcast critical information by means such as text messaging to multiple organizations.
35. Formatting  
Ability to effectively and efficiently exchange data between agencies/jurisdictions (e.g., by employing common data representation structures and exchange formats and protocols).
36. Open Source Formatting  
Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by encouraging open source format.
37. Data Security  
Capability of maintaining the security requirements of any entity within a broader security framework.
38. Field Image Capture and Distribution  
Capability of field image capture and distribution.
39. Data Access to Background Information Sources  
Ability to access information related to hazardous materials, water sources, floor and building plans, fire pre-plans, utility maps, weather forecasts, topographic terrain, transportation, and other background data to support public safety incident management.
40. Data Access to Medical Information  
Ability to manage medical information.
41. Data Access to Legal Information  
Ability to access legal information such as investigation/litigation records, court scheduling records, disposition data and charge data.

Note: Includes extracts from SAFECOM/AGILE/NIST Summit on Interoperable Communications for Public Safety, held at the National Institute of Standards and Technology (NIST)

## Appendix 3 - Evolving Systems Engineering Management Plan Considerations

(an extract from the System of Systems Preliminary Draft Project Plan)

Numerous plans are prepared to define which technical activities will be conducted. They address the integration of engineering specialties requirements, “design-for” requirements, and resource requirements, and discuss how progress toward system level goals will be measured. The Systems Engineering Management Plan (SEMP) is the key planning document which reflects these requirements. The PSRSPC proposes to use the SEMP as its basic plan governing the systems engineering effort for the SoS Project. The SEMP is a concise, top level, technical management plan for the integration of all systems engineering activities. Systems engineering is composed of two components; systems engineering management and the systems engineering process. Both are implemented through the SEMP.

The PSRSPC’s SEMP should contain the following elements:

### ***Part I: Technical Program Planning and Control:***

*Identifies PSRSPC’s organizational responsibilities and authority for systems engineering management; PSRSPC’s control of subcontracted engineering, verification, configuration management, and technical document & data management; and the proposed plans and schedules for technical design and program reviews. The PSRSPC should propose to cover the following areas in Part I of the SEMP:*

- Responsibilities and Authority
- Standards, Procedures, and Training
- Program Risk Analysis
- Engineering Program Integration
- Contract Work Breakdown Structure
- Assessment of Responsibility and Authority
- Program Reviews
- Technical Design Reviews
- Engineering Program Integration
- Technical Performance Measurement
- Change Control Procedures
- Interface Control
- Documentation Control
- Milestones/Schedule
- Plan for other related technical and program management tasks

### ***Part II: System Engineering Process:***

Describes the PSRSPC's proposed systems engineering process used in defining the system design and test requirements. In Part II, the PSRSPC should include the specific customization of the process to requirements of the system; procedures to be used in implementing the process; trade study methodology; types of mathematical or simulation models to be used for system and cost effectiveness evaluations; generation of specifications; generation of applicable engineering documentation. The PSRSPC should cover the following areas in Part II of the SEMP:

- Mission and Requirements Analysis
- Functional Analysis
- Requirements Allocation
- Trade Studies
- Design Optimization
- Design Effectiveness Analysis
- Conceptual Design
- Technical Interface Compatibility
- Logistics Support Analysis
- Producibility Analysis
- Specification Tree/Generation of Specifications
- Documentation
- Other related system engineering tasks

***Part III: Engineering Specialty Integration:***

Describes the PSRSPC's proposed efforts to integrate the requirements of the engineering specialties into the mainstream system design effort. The PSRSPC SEMP will cover the following areas:

1. Integration Design/Plans Risk Alleviation

- Reliability
- Maintainability
- Human Engineering
- Producibility
- Standardization
- Survivability/Vulnerability
- Electromagnetic Interference/Compatibility (EMI/EMC)
- Safety
- Integrated Logistics Engineering
- Computer Resources Life Cycle Management Plan
- Environmental Engineering
- Related Areas

2. Integration System Test Plans

### 3. Compatibility with Supporting Activities

- System Cost Effectiveness
- Value Engineering
- TQM/Quality Assurance
- Materials and Processes

Plans the PSRSPC produces under the SEMP should, as a minimum, contain the following systems engineering information:

1. Plan Objective: Purpose and scope
2. Plan Definition: Succinct description of all tasks required to fulfill the specified purpose including inputs and characteristics of outputs.
3. Responsibilities: Delineation of all organizations collaborating on the tasks, the task(s), or portion of the task for which they are responsible, and the line of authority.
4. Schedule of Activities: Sequence and timing of tasks tied to program schedule milestones, showing inputs from collaborating organizations
5. Resource Definition: Inclusive identification of hardware, software, and facilities required to perform the task(s) within the specified time frame

Providing sufficient detail in the plans can minimize the number of problems likely to be encountered in performing the task(s).

### **G. Systems Engineering Summary:**

Implementation of the foregoing process leads to a well-defined, completely documented and optimally balanced system. It does not produce the actual system, but rather does generate the complete set of documentation tailored to the needs of the Phase I project, which fully describes the system to be developed and produced. The PSRSPC should be synchronized with the following objectives throughout the life of the SoS Project:

- Participating agency system and subsystem requirements will be consistent, correlatable, and traceable.
- The philosophy of minimum documentation will be evident.
- Acquisition and operating cost will be an integral part of the evaluation and decision process.
- Baselines will be established progressively as an integral part of the systems engineering process.
- The process will result in a design that is complete, at a given level of detail, from a total system viewpoint.
- The process will provide for the timely and appropriate integration of mainstream engineering with engineering specialties to ensure their influence on system design
- The process will be anticipatory, i.e., it will provide for continuing prediction and demonstration of the anticipated or actual achievement of

the primary technical objectives of the system. Problems and risk areas will be identified in a timely manner.

- Formal technical reviews and audits will be an integral part of the systems engineering process.
- The systems engineering process will be responsive to change.
- Significant engineering decisions will be traceable to the systems engineering activities and associated documentation upon which they were based.

## **Appendix 4 - FCC Licensing Issues Relative to the Use of Gateway Devices**

Prepared by Glen Nash, California Department of General Services, Telecommunications Division

### **BACKGROUND**

Section 301 of the Communications Act of 1934 (47 USC Section 301), as amended, requires all devices that transmit energy, communications or signals by radio be operated in accordance with the Act and with a license granted under the provisions of the Act. The Act then goes on to establish the Federal Communications Commission (FCC) as the responsible Federal agency for granting licenses and gives it power to establish rules, processes, and procedures for the issuance of such licenses. The FCC further is empowered to establish rules regarding the use of radio transmitting devices. The power of the FCC is limited to non-government use of the radio spectrum. In this context, the term “non-government” refers to all users other than agencies of the Federal government. Therefore, state/county/local governmental entities are classified as “non-government” and are subject to the rules and regulations promulgated by the FCC.

The Federal Communications Commission has established a large volume of rules regarding use of the radio spectrum by non-governmental users. These rules cover the full gamut from radio and television broadcast, to cellular telephone, to point-to-point microwave and satellite services, to the land mobile radio communications used by public safety agencies. The operation of “gateway devices” would fall within the area of land mobile radio communications. Part 90 of the FCC Rules and Regulations (47 CFR Part 90) establishes the rules governing the use of radio transmitting devices used for land mobile radio communications and establishes the processes and procedures for licensing such devices.

While gateway devices, in and of themselves, generally are not “radio transmitting devices”, they are intended to control the use and operation of other devices that are “radio transmitting devices”. Therefore, the operation of gateway devices has an impact upon the licensing of those other devices. Furthermore, the restrictions imposed upon the operation of those other devices have an impact on the use of the gateway device by placing restrictions on how it may be used in an operational environment.

Some of the problems related to the use of gateway devices stem from the fact that, when the FCC rules were written/adopted, gateway devices did not exist. Thus, the FCC Rules and Regulations did not contemplate the use of gateway devices and the deployment of such devices poses potential problems. Some of these problems clearly represent violations of the FCC Rules. Others are less clear. It should be noted that a “willful” violation of the FCC Rules and Regulations can lead to a variety of sanctions. These sanctions may vary from a simple order to “don’t do it again” to the imposition of fines (called forfeitures in the FCC Rules) of as much as \$10,000 per day/per occurrence. In extreme cases, the FCC has made a finding that the individual is “not eligible” to hold any FCC license, thus would be ineligible to operate any sort of radio transmitting device. While such extreme action is unlikely to ever be taken against a state/county/local governmental entity because of the devastating effect it would have on the provision of public safety services (police, fire, EMS, etc.), the FCC will not accept the continued willful violation of its rules.

#### POTENTIAL AREAS OF CONCERN

1. In granting a license, the FCC defines the location at which that license is applicable. For example, a station may be authorized for operation at 1234 Main St, Anywhereville, CA. This station may be operated only at that location and cannot be operated at 1236 Main St (next door) without violating the conditions of the license. While the FCC Rules do not specify the exact level of accuracy required in defining the location of a transmitter, the location is defined on the license in terms of latitude/longitude with an apparent accuracy of 1/10<sup>th</sup> second of arc (which equates to +/- about 10 feet). This level of accuracy is difficult to attain without having a land surveyor conduct a formal survey of the antenna location. In practicality, most licensees adhere to an accuracy of 1 second of arc (about 100 feet).

Obviously, not all radio transmitters are intended to operate at only one location. Thus, while the stations described above are known as “fixed stations”, there are separate classes of stations that are allowed to move about within a defined “operational area”. Generally, these stations are called “mobile” stations. These include handheld portable radios and radios installed in some sort of vehicle. It also includes a special class of fixed station known as a “temporary fixed station”. In appearance and operation, “temporary fixed stations” are identical to a “fixed station”. The difference lies in the fact that the “temporary fixed station” is being used at any particular fixed location for less than 180 days. Typically, the FCC defines the operational area for a mobile or “temporary fixed station” in fairly broad terms (e.g. “Statewide—California” or “Countywide---Los Angeles County, CA” or “30-mile radius around Point A” where Point A is defined in terms of a latitude/longitude”).

The potential problem arising from the use of gateway devices relates to where the device (and its associated radios) is relative to the operational area defined for the associated radios. If the FCC license for a particular radio frequency defines

the operational area as “Countywide---Los Angeles County”, then that frequency cannot be used in San Bernardino County under that license without violating the conditions of the license. Thus, the operator of a gateway device must be aware of the geographic conditions placed on every license he/she intends to use in activating the gateway device as well as the location at which he/she intends to operate to ensure that he/she is in full compliance with the license requirements.

The “obvious solution” to this problem is for the State of California to obtain a license on every potential frequency that might be implemented in a gateway device and to have that license define the operational area as “Statewide---California”. Ignoring the potential for a need to operate in an adjoining state, this solution has another significant drawback. Such a license would require that each of the county/local entities on whose “frequency” the device were to be used would have to grant “permission” for the State to have such a license (this “permission” results from a requirement for “frequency coordination” that is intended to minimize interference between different user agencies). Most county/local governmental agencies are reluctant to grant such permission because of the potential interruption to their critical operations if interference were to occur. In fact, the indiscriminate implementation of gateway devices in some parts of California (and at the scene of some incidents) already has resulted in disruptive interference that has negatively impacted normal day-to-day operations. For this reason, operational commanders are very reluctant to grant broad authority to use “their frequencies”.

To resolve this potential problem, the agency operating the gateway device must do all of the following:

- a. Determine which frequencies upon which the device will be “equipped” to operate. Even though most of today’s synthesized radios can be programmed to operate on a wide variety of frequencies, the channels actually programmed into the radios associated with the gateway device (thus available to the operator of the gateway) will have to be limited to those defined in this step.
- b. Appropriate FCC licenses authorizing operation of the frequencies defined above will have to be obtained. This might be accomplished by obtaining a letter of authorization for the device to be operated under the FCC license held by some other entity. To the extent that a new FCC license will be acquired, then all of the processes/procedures associated with obtaining that license must be followed. This includes the “frequency coordination” process, in which incumbent users of a given frequency have an opportunity to comment on the proposed “new use”. All such comments must be resolved prior to the license application being forwarded to the FCC. Based on past experience, obtaining the necessary concurrences from incumbent licensees can be a daunting task.
- c. Guidelines will have to be written which describe what frequencies may be used and the conditions under which those frequencies can be used.

These guidelines should include any restrictions limiting the geographic area in which the frequency may be used, the operational conditions under which it might be used, and any requirement for notifying other users prior to use. A process for regular review and updating of the guidelines should be implemented.

- d. Operators of the gateway device will have to be educated on the use of the guidelines. Regular training exercises are highly recommended.
  - e. Use of the guidelines must be strictly enforced. Failure to do so could result in disruptive interference to vital public safety operations during a time of great need.
2. The appropriate manner in which to obtain an FCC license for the radios associated with the gateway device may present a problem. This potential problem relates to the fact that gateway devices did not exist when the FCC Rules and Regulations were written, thus the devices do not clearly fit within one of the standard classifications for transmitting devices. DGS-TD understands that this question has been posed to the FCC, but that no definitive answer has been provided.

When licensed, radios are “classified” based upon their intended operation. As noted above, some radios might be classified as “mobile radios” while others are classified as “fixed stations”. There are specific differences in how some of the other FCC rules are implemented dependent upon how the radio is classified. For example, the frequencies that might be available for licensing are different for different “classes” of fixed station.

”Mobile” radios generally have the greatest flexibility as to what frequencies are available for licensing and where the radio might be operated. However, “mobile” radios generally are perceived as devices that a person operates. The transmitter is “keyed on” through the use of a “push-to-talk” switch on the radio that is depressed by the operator. The radio is modulated by the operator speaking into a microphone that is integral to the radio. The radios used by gateway devices may have been designed by the manufacturer to be a “mobile” radio, but their functional implementation does not satisfy these traditional definitions. The radio is not “keyed on” by the operation of a “push-to-talk” switch, but rather is automatically “keyed on” by the reception of a signal at the receiver of another radio connected to the gateway device. The radio is not modulated by a person speaking into an integral microphone, but rather is automatically modulated by the signal output from the receiver from another radio connected to the gateway device. Thus, once the gateway device is set-up, there is no requirement that a person operate the associated radios. This mode of operation is more akin to a mode described in the FCC Rules as a “mobile relay” mode of operation.

Furthermore, gateway devices installed at fixed locations suffer from a more direct classification problem. “Mobile radios” are intended to be just that,

mobile. They are expected to be a single location for a matter of minutes, perhaps hours or days, but certainly not months or years. Devices that remain at one location for a long period of time are classified under one of a series of “fixed” classifications, dependent on how the radio is used. These classifications include “mobile relay”, “control station” and “base station”.

While “classifying” the radios associated with a gateway device as “mobile relays” may answer one question, it creates new questions and concerns. The FCC Rules include certain restrictions relative to the frequencies on which a “mobile relay” may operate. Once again, when the FCC Rules were written, “mobile relays” were intended to be radios placed at high locations such that they could “repeat” the signal coming from one subscriber unit out over a wide area such that it could be heard by a large number of subscriber units. In an effort to organize how the overall radio spectrum was utilized, certain frequencies were defined as available for the “inbound” (or “uplink”) signal from the originating subscriber unit to the mobile relay and other frequencies were defined as available for the “outbound” (or “downlink”) signal from the mobile relay to the “listening” subscriber units. Specific “inbound” frequencies were paired with specific “outbound” frequencies to create what are known as “repeater pairs”. The problem with a gateway device is that, typically, it operates by taking the audio associated with the “outbound” channel on one repeater pair and connects it to the “inbound” channel of one or more other repeater pairs. Thus, not only are the radios associated with the gateway device operating in a manner “opposite” to the way a mobile relay typically operates, but it also is not “repeating” on standard repeater pairs.

There is another “class” of fixed station that is intended to operate in a manner similar to that in which the radios associated with the gateway device are intended to operate, i.e. transmitting on the “inbound” channel and receiving on the “outbound” channel of a repeater pair. This class is known as a “control station”. However, like the mobile radio, this class of station is intended to interface with a human being and is not described in the FCC Rules as including the “automatic retransmission” feature of the gateway device.

There is no clear solution to this potential problem. Whatever course of action an agency may follow, the FCC may determine at some future date that a different course of action would have been more appropriate. But---failing to obtain a license at all may be perceived as an “intent to commit a willful violation” of the FCC Rules, whereas, obtaining a license that improperly defines the mode of operation would be perceived simply as a “violation” of the FCC Rules. Furthermore, this simple “violation” might be mitigated by an argument similar to that described above, in which it is shown that the Rules were/are unclear and that the State had attempted to act in responsible manner.

Thus, to resolve this problem, DGS-TD recommends that, for whatever frequencies are programmed into the radios associated with the gateway devices,

such use be based upon FCC licenses showing “mobile” as the mode of operation. In circumstances wherein the gateway device is installed at a fixed location, then the FCC license should be based upon operation at that fixed location and should show a either a “base station” or a “control station” mode of operation, as appropriate for the frequencies being implemented.

3. The Communications Act of 1934 and the FCC Rules and Regulations contain a general prohibition against willfully causing interference to other licensed users of the radio spectrum. Users of gateway devices need to be cautious with regard to this requirement. The devices are capable of linking a wide variety of frequencies as a means of enhancing interoperability. But, they also can create monstrous interference problems if not properly used. Potential problems include:
  - a. Linking together groups of users who have no need or desire to be linked together, thereby causing each group to receive “interference” from the other.
  - b. Conducting operations on a channel that also is used in a nearby area by some other agency that is not a part of the mutual aid event. This could result in that other entity receiving unacceptable interference to their normal day-to-day operations on that frequency and may render the frequency useless until the interference is resolved.
  - c. Conducting operations on a channel that is used by one of the participants in the mutual aid event, but is not the channel that they want used for that purpose. As described in “b” above, this could render the affected channel useless for its normal day-to-day purpose. This situation could arise from a failure to keep the operational guidelines up-to-date. For example, when the guidelines were written, the affected agency may have wanted mutual aid operations to occur on that channel. However, they subsequently made changes to their overall radio system and now would want mutual aid operations to occur on a different channel. If the guidelines had not been reviewed and updated to reflect this change, unacceptable interference to the affected agency could result.
  - d. Based upon the selection of frequencies upon which the radios associated with the gateway device operate and how those radios/antennas are installed, it is possible that inter-modulation products could be created that cause interference problems to other nearby systems. They also could cause the gateway device to go into a “feedback loop”.
  - e. Multiple gateway devices deployed to the same event could interact with each other, thereby causing unacceptable interference.

## Appendix 5- PSRSPC Statute as of January 1, 2007

### GOVERNMENT CODE SECTION 8592-8592.7

8592. This article shall be known and may be cited as the Public Safety Communication Act of 2002.

8592.1. For purposes of this article, the following terms have the following meanings:

(a) "Backward compatibility" means that the equipment is able to function with older, existing equipment.

(b) "Committee" means the Public Safety Radio Strategic Planning Committee, which was established in December 1994 in recognition of the need to improve existing public radio systems and to develop interoperability among public safety departments, and between state public safety departments and local or federal entities and which consists of representatives of the following state entities:

- (1) The Office of Emergency Services, who shall serve as chairperson.
- (2) The California Highway Patrol.
- (3) The Department of Transportation.
- (4) The Department of Corrections and Rehabilitation.
- (5) The Department of Parks and Recreation.
- (6) The Department of Fish and Game.
- (7) The Department of Forestry and Fire Protection.
- (8) The Department of Justice.
- (9) The Department of Water Resources.
- (10) The State Department of Health Services.
- (11) The Emergency Medical Services Authority.
- (12) The Department of General Services.
- (13) The Office of Homeland Security.
- (14) The Military Department.
- (15) Department of Finance.

(c) "First response agencies" means public agencies that, in the early stages of an incident, are responsible for, among other things, the protection and preservation of life, property, evidence, and the environment, including, but not limited to, state fire agencies, state and local emergency medical services agencies, local sheriffs' departments, municipal police departments, county and city fire departments, and police and fire protection districts.

(d) "Nonproprietary equipment or systems" means equipment or systems that are able to function with another manufacturer's equipment or system regardless of type or design.

(e) "Open architecture" means a system that can accommodate equipment from various vendors because it is not a proprietary system.

(f) "Public safety radio subscriber" means the ultimate end user. Subscribers include individuals or organizations, including, for example, local police departments, fire departments, and other operators of a public safety radio system. Typical subscriber equipment includes end instruments, including mobile radios, hand-held radios, mobile

repeaters, fixed repeaters, transmitters, or receivers that are interconnected to utilize assigned public safety communications frequencies.

(g) "Public safety spectrum" means the spectrum allocated by the Federal Communications Commission for operation of interoperable and general use radio communication systems for public safety purposes within the state.

8592.2. (a) The committee shall have primary responsibility in state government for both of the following:

(1) Developing and implementing a statewide integrated public safety communication system that facilitates interoperability among state public safety departments listed in subdivision (b) of Section 8592.1 and other first response agencies, as the committee deems appropriate.

(2) Coordinating other shared uses of the public safety spectrum consistent with decisions and regulations of the Federal Communications Commission.

(b) In order to facilitate effective use of the public safety spectrum, the committee shall consult with any regional planning committee or other federal, state, or local entity with responsibility for developing, operating, or monitoring interoperability of the public safety spectrum.

(c) The committee shall meet at least twice a year, of which one meeting shall be a joint meeting with the California Statewide Interoperability Executive Committee to enhance coordination and cooperation at all organizational levels and a cohesive approach to communications interoperability.

8592.3. (a) The committee shall consult with the following organizations and entities:

- (1) California State Peace Officers Association.
- (2) California Police Chiefs Association.
- (3) California State Sheriffs' Association.
- (4) California Professional Firefighters.
- (5) California Fire Chiefs Association.
- (6) California State Association of Counties.
- (7) League of California Cities.
- (8) California State Firefighters Association.
- (9) California Coalition of Law Enforcement Associations.
- (10) California Correctional Peace Officers Association.
- (11) CDF Firefighters.
- (12) California Union of Safety Employees.

(b) Each organization or entity listed in subdivision (a) may designate a representative to work with the committee to develop agreements for interoperability or other shared use of the public safety spectrum between the state public safety departments listed in subdivision (b) of Section 8592.1 and local or federal agencies that operate a communication system on the public safety spectrum and that have capacity and technical ability for interoperability or other shared use.

(c) The committee shall develop a model memorandum of understanding that sets forth general terms for interoperability or other shared uses among jurisdictions, which may be modified as necessary for a particular agreement entered into pursuant to subdivision (b).

(d) A local agency may not be required to adopt the model memorandum of understanding developed pursuant to subdivision (c).

8592.4. (a) The committee shall determine which state public safety departments listed in subdivision (b) of Section 8592.1 need new or upgraded communication equipment and shall establish a program for equipment purchase. In establishing this program, the committee shall recommend the purchase of public safety radio subscriber equipment that will enable state agencies to commence conforming to industry and governmental standards for interoperability as set forth in Section 8592.5. As technology continues to evolve, the committee shall recommend the purchase of nonproprietary equipment or systems that have open architecture and backward compatibility, and that are in compliance with paragraphs (1) and (2) of subdivision (a) of Section 8592.5.

(b) The committee may recommend to any other federal, state, regional, or local entity with responsibility for developing, operating, or monitoring interoperability of the public safety spectrum, the purchase of public safety radio subscriber equipment that will enable first response agencies to commence conforming to industry and governmental standards for interoperability as set forth in paragraphs (1) and (2) of subdivision (a) of Section 8592.5. As technology continues to evolve, the committee may recommend the purchase of nonproprietary equipment or systems that have open architecture and backward compatibility, and that are in compliance with paragraphs (1) and (2) of subdivision (a) of Section 8592.5.

(c) This section may not be construed to mandate that a state or local governmental agency affected thereby is required to compromise its immediate mission or ability to function and carry out its existing responsibilities.

8592.5. (a) Except as provided in subdivision (c), a state department that purchases public safety radio communication equipment shall ensure that the equipment purchased complies with applicable provisions of the following:

(1) The common system standards for digital public safety radio communications commonly referred to as the "Project 25 Standard," as that standard may be amended, revised, or added to in the future jointly by the Associated Public-Safety Communications Officials, Inc., National Association of State Telecommunications Directors and agencies of the Federal Government, commonly referred to as "APCO/NASTD/FED."

(2) The operational and functional requirements delineated in the Statement of Requirements for Public Safety Wireless Communications and Interoperability developed by the SAFECOM Program under the United States Department of Homeland Security.

(b) Except as provided in subdivision (c), a local first response agency that purchases public safety radio communication equipment, in whole or in part, with state funds or federal funds administered by the state, shall ensure that the equipment purchased complies with paragraphs (1) and (2) of subdivision (a).

(c) Subdivision (a) or (b) shall not apply to either of the following:

(1) Purchases of equipment to operate with existing state or local communications systems where the latest applicable standard will not be compatible, as verified by the Telecommunications Division of the Department of General Services.

(2) Purchases of equipment for existing statewide low-band public safety communications systems.

(d) This section may not be construed to require an affected state governmental agency to compromise its immediate mission or ability to function and carry out its existing responsibilities.

8592.6. (a) The committee shall report to the Legislature by January 1 of each year on the committee's progress in implementing this article.

(b) (1) The annual report shall serve as the state's strategic plan to establish a statewide integrated, interoperable public safety communications network. The report shall include, but not be limited to, implementation strategies and timelines to achieve the goals and objectives set forth in the report. The implementation strategies and timelines may include identification of resource needs, including data formats, possible funding sources, prioritization of expenditures, and the development of common protocols that build upon industry and governmental standards for interoperability as set forth in paragraphs (1) and (2) of subdivision (a) of Section 8592.5 that will advance the integration of local, regional, and statewide interoperable public safety communication networks. The report shall be updated annually, as strategies, timelines, goals, and objectives are accomplished or changed.

(2) In developing the report, the committee, at its discretion, shall consult with any other local, regional, state, or federal entity with responsibility for developing, operating, or monitoring interoperability of the public safety spectrum, and other first response agencies. The report may include recommendations for local, regional, state, or federal entities to coordinate resources and the development of common protocols to advance the integration of local, regional, and statewide interoperable public safety communication networks.

(c) The report will include a complete listing of purchases by state departments of public safety radio communications equipment, for which a waiver of subdivision (a) of Section 8592.5 was granted by the committee.

8592.7. (a) A budget proposal submitted by a state agency for support of a new or modified radio system shall be accompanied by a technical project plan that includes all of the following:

- (1) The scope of the project.
- (2) Alternatives considered.
- (3) Justification for the proposed solution.
- (4) A project implementation plan.
- (5) A proposed timeline.
- (6) Estimated costs by fiscal year.

(b) The committee shall review the plans submitted pursuant to subdivision (a) for consistency with the statewide integrated public safety communication strategic plan included in the annual report required pursuant to Section 8592.6.

(c) The Telecommunications Division of the Department of General Services shall review the plans submitted pursuant to subdivision (a) for consistency with the technical requirements of the statewide integrated public safety communication strategic plan included in the annual report required pursuant to Section 8592.6.

## **Appendix 6 - Public Safety Radio Strategic Planning Committee resolution regarding compliance with TIA-102/APCO Project 25 standards (September 22, 2006)**

### **BACKGROUND:**

California Government Code Section 8592 states the following:

8592. This article shall be known and may be cited as the Public Safety Communication Act of 2002.

8592.1. For purposes of this article, the following terms have the following meanings:

(a) "Public safety spectrum" means the spectrum allocated by the Federal Communications Commission for operation of interoperable and general use radio communication systems for public safety purposes within the state.

(b) "Committee" means the Public Safety Radio Strategic Planning Committee, which was established in December 1994 in recognition of the need to improve existing public radio systems and to develop interoperability among public safety departments, and between state public safety departments and local or federal entities and which consists of representatives of the following state entities:

- (1) The California Highway Patrol.
- (2) The Department of Transportation.
- (3) The Department of Corrections.
- (4) The Department of Parks and Recreation.
- (5) The Department of Fish and Game.
- (6) The Department of Forestry and Fire Protection.
- (7) The Department of Justice.
- (8) The Department of Water Resources.
- (9) The Office of Emergency Services.
- (10) The Emergency Medical Services Authority.
- (11) The Department of the Youth Authority.
- (12) The Department of General Services.
- (13) The Office of Homeland Security.

8592.2. (a) The committee shall have primary responsibility in state government for developing and implementing a statewide integrated public safety communication system that facilitates interoperability among state public safety departments listed in subdivision (b) of Section 8592.1 and coordinates other shared uses of the public safety spectrum consistent with decisions and regulations of the Federal Communications Commission. In order to facilitate effective use of the public safety spectrum, the committee shall consult with any regional planning

committee or other federal, state, or local entity with responsibility for developing, operating, or monitoring interoperability of the public safety spectrum.

(b) The committee shall elect from among its members a chair with responsibility for leadership in implementing this article.

8592.3. (a) The committee shall consult with the following organizations and entities:

- (1) California State Peace Officers Association.
- (2) California Police Chiefs Association.
- (3) California State Sheriffs' Association.
- (4) California Professional Firefighters.
- (5) California Fire Chiefs Association.
- (6) California State Association of Counties.
- (7) League of California Cities.
- (8) California State Firefighters Association.
- (9) California Coalition of Law Enforcement Associations.
- (10) California Correctional Peace Officers Association.
- (11) CDF Firefighters.
- (12) California Union of Safety Employees.
- (13) The Military Department.

(b) Each organization or entity listed in subdivision (a) may designate a representative to work with the committee to develop agreements for interoperability or other shared use of the public

safety spectrum between the state public safety departments listed in subdivision (b) of Section 8592.1 and local or federal agencies that operate a communication system on the public safety spectrum and that have capacity and technical ability for interoperability or other shared use.

(c) The committee shall develop a model memorandum of understanding that sets forth general terms for interoperability or other shared uses among jurisdictions, which may be modified as necessary for a particular agreement entered into pursuant to subdivision (b).

(d) A local agency may not be required to adopt the model memorandum of understanding developed pursuant to subdivision (c).

8592.4. (a) The committee shall determine which state public safety departments listed in subdivision (b) of Section 8592.1 need new or upgraded communication equipment and shall establish a program for equipment purchase. In establishing this program, the committee shall recommend the purchase of equipment that will enable state agencies to commence conforming to accepted industry standards for interoperability specified in subdivision (a) of Section 8592.5.

(b) This section may not be construed to mandate that a state or local governmental agency affected thereby is required to compromise its immediate mission or ability to function and carry out its existing responsibilities.

8592.5. (a) Except as provided in subdivision (b), a state department that purchases public safety radio communication equipment shall ensure that the equipment purchased complies with applicable provisions of the following:

(1) The common system standards for digital public safety radio communications commonly referred to as the "Project 25 Standard," as that standard may be amended, revised, or added to in the future jointly by the Associated Public-Safety Communications Officials, Inc., National Association of State Telecommunications Directors and agencies of the Federal Government, commonly referred to as "APCO/NASTD/FED."

(2) The operational and functional requirements delineated in the Statement of Requirements for Public Safety Wireless Communications and Interoperability developed by the SAFECOM Program under the United States Department of Homeland Security.

(b) Subdivision (a) shall not apply to either of the following:

(1) Purchases of equipment to operate with existing state or local communications systems where the latest applicable standard will not be compatible, as verified by the Telecommunications Division of the Department of General Services.

(2) Purchases of equipment for existing statewide low-band public safety communications systems.

(c) This section may not be construed to require an affected state governmental agency to compromise its immediate mission or ability to function and carry out its existing responsibilities.

8592.6. (a) The committee shall report to the Legislature by January 1 of each year on the committee's progress in implementing this article.

(b) The report will include a complete listing of purchases by state departments of public safety radio communications equipment, for which a waiver of subdivision (a) of Section 8592.5 was granted by the committee.

8592.7. (a) A budget proposal submitted by a state agency for support of a new or modified radio system shall be accompanied by a technical project plan that includes all of the following:

- (1) The scope of the project.
- (2) Alternatives considered.
- (3) Justification for the proposed solution.
- (4) A project implementation plan.
- (5) A proposed timeline.
- (6) Estimated costs by fiscal year.

(b) The committee shall review the plans submitted pursuant to subdivision (a) for consistency with the statewide integrated public safety communication strategic plan included in the annual report required pursuant to Section 8592.6.

(c) The Telecommunications Division of the Department of General Services shall review the plans submitted pursuant to subdivision (a) for consistency with the technical requirements of the statewide integrated public safety communication strategic plan included in the annual report required pursuant to Section 8592.6.

Government Code Section 14931 gives the Department of General Services (DGS) the authority to purchase public safety equipment for state agencies as follows:

14931. The department may acquire, install, equip, maintain, and operate new or existing communications systems and facilities. To accomplish that purpose, it may, in the name of the state, enter into contracts, obtain licenses, acquire property, install necessary equipment and facilities, and do such other acts as will provide adequate and efficient communications systems. Any system established shall be available to all public agencies in the state on such terms as may be agreed upon by the agency and the department.

Recent attempts by DGS to purchase equipment that meets the latest “Project 25 standard” as required by section 8592 (a)(1) have resulted in non-compliant bids being received from manufacturers. In particular, manufacturers and vendors have been unable to supply equipment compliant with the TIA-102.BAHA “Fixed Station Interface” standard adopted June, 2006. At the time of bid opening and evaluation, no manufacturers who responded were capable of supplying equipment that would comply with this requirement. This was attributed to development and manufacturing lead time associated with tooling up to meet a newly-adopted standard.

The various documents that summarize the Project 25 Statement of Requirements have generally recognized the lag time between adoption of a standard and the availability of products on the market that meet that standard. This resolution allows the Department of General Services the flexibility to adopt new standards into product specifications as market surveys show the ability of manufacturers and vendors to provide compliant products.

## **RESOLUTION:**

Whereas:

- The California Public Safety Radio Strategic Planning Committee is committed to meeting the requirements of California Government Code Section 8592 et. seq., also known as the “Public Safety Communication Act of 2002”;
- The California Public Safety Radio Strategic Planning Committee recognizes that there is a lag time between the adoption of a “Project 25” standard by the Telecommunications Industry Association (TIA) and the availability of compliant products from manufacturers and vendors;
- The Department of General Services (DGS) is tasked by Government Code Section 14931 to procure public safety communications equipment and has the procedures in place to perform market surveys of available equipment that will comply with “Project 25” standards while developing standards for the procurement of that equipment;
- The California Public Safety Radio Strategic Planning Committee recognizes that some manufacturers and vendors of public safety communications equipment develop products faster than others.

Be it resolved that:

- The California Public Safety Radio Strategic Planning Committee grants the Department of General Services the flexibility to first ensure availability of equipment that complies with “Project 25” standards before incorporating those standards into an equipment purchase specification. The method of determining the availability of such equipment will be the normal market survey process currently conducted by DGS before each Invitation for Bid. Should this survey determine that no manufacturer or vendor will be able to bid a product that complies with this standard, DGS shall have the ability to not include that standard in a procurement specification.
- The California Public Safety Radio Strategic Planning Committee directs the Department of General Services that should they find, during the market survey referenced above, only one manufacturer or vendor capable of supplying a “Project 25” product compliant with the most recently revised or amended standards, DGS shall have the ability to include those requirements into a bid specification and shall recognize that this situation will not result in the bid being characterized a “Non-Competitive Bid”.

DRAFT