California Interoperability:

Introductory Information

Version 10/13/06

Compiled by: California Statewide Interoperability Executive Committee (CALSIEC) and Public Safety Radio Strategic Planning Committee (PSRSPC) members

After meeting with representatives of several state and local agencies with a stake in the interoperability of California, it has come to our attention that much like our communication systems, the familiarity with interoperability efforts within the state can vary from person to person, and agency to agency. For this reason, we have compiled this grouping of short documents to provide a base of common knowledge regarding the current and future efforts put forth by local, state, and federal agencies regarding interoperable communications within the state of California. Each excerpted document contains basic information regarding its specific topic, and in the table of contents, the origination of the document is listed for further research if desired. We hope that this will help in providing information that we can all use in making our meetings more productive and efficient in aims of improving communication among first responders in the state of California.

Thanks,

California's Office of Homeland Security on behalf of Planning Area Development Team of the California Statewide Interoperability Executive Committee in partnership with the Public Safety Radio Strategic Planning Committee.

TABLE OF CONTENTS

Topical Web Site References ... 3
Interoperability Defined ... 4
Background of California Interoperability ... 4
Background and Context ... 4
Emergency Management Systems ... 5
Frequency Spectrum ... 6
California is a Patchwork of Communications Systems ... 6
Regional Systems ... 6
Current Status of Interoperability Technology ... 7
Partner Organizations-Federal and State ... 7
SAFECOM Overview ... 9
Mission ... 9
Governance ... 9
Initiatives ... 9
SAFECOM Further Explained: Frequently Asked Questions of SAFECOM ... 11
ICTAP Overview ... 14
Interoperable Communications Technical Assistance Program (ICTAP) ... 14
ICTAP Further Explained: Frequently Asked Questions of ICTAP ... 15
TICP Overview ... 17
Tactical Interoperable Communications Plan Guidance ... 17
TICPs Further Explained: Frequently Asked Questions of TICPs ... 18
Gateways Explained ... 21
PSRSPC Overview ... 26
The PSRSPC Work Effort ... 26
CALSIEC Overview ... 27
A Potential Executive Committee and Subcommittee Template for Northern, Capitol/Bay Area, and Central CALSIEC Planning Areas ... 27
TABLE: Counties by CalSIEC Planning Area ... 28
MAP: California Statewide Interoperable Executive Committee Planning Areas ... 29
MAP: OES Administrative Regions with Mutual Aid Regions ... 30
The $1million Question: ... 31

Topical Web Site References

Interoperability Defined
Definition as Taken from SAFECOM Website:
http://www.safecomprogram.gov/SAFECOM/interoperability/default.htm

Background of CA Interoperability
Excerpted from 2006 PSRSPC Report to the Legislature:
http://psrspc.ca.gov/lib/2006_Report.pdf

SAFECOM Overview
Excerpted from SAFECOM Program Website:
http://www.safecomprogram.gov/SAFECOM/about/default.htm

SAFECOM Further Explained: FAQ's
Excerpted from SAFECOM Program Website:
http://www.safecomprogram.gov/SAFECOM/about/default.htm

ICTAP Overview
Excerpted from Department of Homeland Security (DHS) Grants and Training Website:
http://www.ojp.usdoj.gov/odp/ta_ictap.htm

ICTAP Further Explained: FAQ's
Excerpted from "ODP Tactical Interoperable Communication Plan Frequently Asked Questions":
http://www.ojp.usdoj.gov/odp/docs/TICP_FAQ.pdf

TICP Overview
Excerpted from DHS' "Tactical Interoperable Communications Planning Guidance and Template":
http://www.ojp.usdoj.gov/odp/docs/TICPGuidanceandTemplate.pdf

TICPs Further Explained: FAQ's
Excerpted from "ODP Tactical Interoperable Communication Plan Frequently Asked Questions":
http://www.ojp.usdoj.gov/odp/docs/TICP_FAQ.pdf

Gateways Explained
Article: "Gateways-the Good, the Bad, the Ugly" : By: Capt. Eddie Reyes, Sponsored by Cisco Systems

PSRSPC Overview
Excerpted from the PSRSPC Website & PSRSPC 2006 Report to the Legislature:
http://psrspc.ca.gov/; http://psrspc.ca.gov/lib/2006_Report.pdf

CALSIEC Overview/Committee Template/Area Breakdowns
Excerpted from the CALSIEC Website:
http://www.calsiec.org/

The $1 Million Question: Why PSRSPC & CALSIEC?
Excerpted from the CALSIEC Website:
http://www.calsiec.org/faq.html

Interoperability Defined

What is communications interoperability?

In general, interoperability refers to the ability of emergency responders to work seamlessly with other systems or products without any special effort. Wireless communications interoperability specifically refers to the ability of emergency response officials to share information via voice and data signals on demand, in real time, when needed, and as authorized. For example, when communications systems are interoperable, police and firefighters responding to a routine incident can talk to each other to coordinate efforts. Communications 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 or an inauguration, or for disaster relief and recovery efforts.

What are the components of a truly interoperable communications system, and what are the barriers to creating one?

There are a variety of challenges to interoperability: some are technical, some financial, and some stem from human factors such as inadequate planning and lack of awareness of the real importance of interoperability.

According to a report published in February 2003 by the National Task Force on Interoperability, the emergency response community views the following as the key issues hampering emergency response wireless communications:

- Incompatible and aging communications equipment;
- Limited and fragmented budget cycles and funding;
- Limited and fragmented planning and coordination;
- Limited and fragmented radio spectrum; and
- Limited equipment standards.

Background of California Interoperability

Background and Context

California's public safety and public service agencies provide a wide range of support including law enforcement, fire protection, disaster response, transportation management, flood control, water conveyance and storage, criminal detention and rehabilitation, search and rescue, and other services to over 34 million residents and 44 million visitors to the State each year. In order to effectively and responsively provide these services, the State's public safety agencies must be able to:

- dispatch work assignments to field personnel;
- receive information about situations in the field from field personnel;
- provide immediate field access to information such as warrants, vehicle registrations, terrain access, missing persons, and gun registrations; and,
- determine the need for, and then provide, additional resources in response to field situations.

Communications is the mechanism by which state managers exercise command and control over their personnel and equipment in response to various situations. For the over 43,000 State public safety employees involved with field operations, mobile radio voice and data communications is the primary, and sometimes only link, to this information and additional resources during both routine and emergency operations. During disasters, such as California's frequent wildfires, the

interoperability of communications systems becomes especially critical since multiple agencies and organizations are routinely called upon for emergency response.

The Department of Homeland Security's SAFECOM program has described the lack of communications interoperability as an issue at the national level. The same may be said of the state of California systems; California is heavily invested in an existing infrastructure that is largely incompatible. Local and federal communications systems in the state exhibit the same incompatibilities.

Among the findings, the PSRSPC has also identified an "operability" problem among California's public safety agencies. Many existing state agency systems have considerable deficiencies in their communications structure and need funding to purchase new systems. While interoperability is the end goal, it is important not to lose sight that agencies must first be able to communicate within their own system structures.

Much work has been done by SAFECOM and its federal partners in defining the requirements that public safety agencies should adopt. More specifically, this report endorses the "Statement of Requirements for Public Safety Wireless Communications and Interoperability" released by the Department of Homeland Security. It is PSRSPC's recommendation that any public safety communications equipment purchased by the State follow the Statement of Requirements document released by SAFECOM.

Emergency Management Systems

Communications interoperability is supported by established emergency management systems within California. Without the emergency management structure, interoperability cannot be accomplished. Successful communications interoperability is contingent upon the fusion of both the technical and organizational aspects. A key component of California's emergency management system is the Incident Command System (ICS), which is the outgrowth of the experiences from the fire services in dealing with wildland fires. It is a field level emergency management system based on management by objectives and focuses on these five functions: command, operations, planning/intelligence, logistics, and finance/administration. ICS fosters integration of various disciplines (fire and rescue, law enforcement, emergency medical, etc.) into a cohesive emergency response organization. ICS became the backbone for California's Standardized Emergency Management System (SEMS). Because California has such a strong ICS structure we are ahead of many states in how we communicate in a disaster. For an example of how ICS works in interoperability, refer to the multi-discipline/multi-jurisdiction-explosion scenario written by SAFECOM and found in Appendix G.

SEMS incorporates ICS, multi/interagency coordination, mutual aid, and the operational area concept to ensure effective emergency response in California. It permits organizations at all levels to respond to frequent and multiple disasters occurring anytime and anywhere in the state. It also facilitates priority setting, interagency cooperation, and the efficient flow of resources and information. Within SEMS there are five organizational levels: field, local, operational area, regional, and state.

At the federal level, the major important developments of the last several years are the new National Incident Management System (NIMS), the new National Response Plan (NRP), and the integration with SEMS. California's SEMS emergency program was recognized as a standard/ best practice and was used as the model for the new NIMS program. NIMS was released as one of the new federal initiatives in the post 9/11 environments geared towards better national-state-local coordination. As the nuances of NIMS, the complimentary (and also new) National Response Plan (NRP) and soon-to-be released National Preparedness Goal (NPG) are addressed for California compliance, interoperability and other new communications elements will need to be integrated into the state's framework.

Frequency Spectrum

"Spectrum" is how scientists describe the range of electromagnetic radiation that is ever-present around us. This energy is usually measured in cycles per second, known as Hertz or "Hz". At one end of this range are the sounds we can hear (speech, music, etc.) that fall in the audible range. At the other end are visible light, x-rays, and gamma radiation. In the middle of the spectrum is the range of frequencies ("channels") used to transmit radio and television signals.

Under international treaty, use of the radio spectrum is administered at the federal level. Congress has delegated the authority to administer the federal use of spectrum to the National Telecommunications and Information Administration (NTIA) in the U.S. Department of Commerce. Congress has delegated regulatory authority for the non-federal use of the radio spectrum to the FCC. Each of these agencies individually promulgates policies and regulations relating to spectrum use within their respective target audiences.

Public safety's two-way voice and data communications networks are included in the "Private Land Mobile Radio" section of the Code of Federal Regulations (47 CFR Part 90). The public safety services have been allocated operating space in twelve different segments of the radio spectrum (refer to Appendix B).

California is a Patchwork of Communications Systems

Regional, local, and state agency-specific communications systems have been evolving since well before 9/11 in response to basic communications needs. Alliances have been developed through a patchwork, ad-hoc approach that was—quite defensibly—needed to "get the job done." In many cases exceptionally effective systems that integrate equipment and procedures have developed that create interoperable "pockets" around California. The strength in this effort is that significant work has been accomplished in many jurisdictions in California that has added to the state's capabilities. The challenge is that most of these regional/local/agency-specific systems have not been evaluated or developed with a common framework in mind that will allow for quick interoperability, should the need arise. Taken individually, it appears that most of the systems likely fit within commonly accepted parameters of interoperability (P25, SAFECOM, etc.), however, a study has not been undertaken to verify this fact. Possibly even more important than equipment standards are integrated procedural guidelines that govern the linking and integration of these different systems when joined in an emergency. The CALSIEC mission addresses many of these questions at a local/regional level; PSRSPC is undertaking this effort as well from a state agency perspective. In both circumstances there is a need to honor the time and money already invested by state agencies and local governments alike.

Regional Systems

Over the last several years, many sophisticated regional programs have emerged as true examples of interoperability within California. Below are excerpts on several of these important programs. (More detailed descriptions can be found in Appendix D). These systems reflect a trend toward a regional/local-centered focus for communications modernization and interoperability. With these regional collaborations now in existence, California's challenge becomes a need to "tie together" these existing regional programs, while supporting their ongoing development according to consistent standards. At the same time, state agency modernization that will assist interfacing between state and local programs is a priority. The following are a few examples of regional programs.

- The California Department of Forestry and Fire Protection (CDF) communications system successfully operates daily in mutual aid radio operations across the state, providing services to local government contracts in 36 counties. All of the CDF

mobile and handheld radios are programmed for compatibility with the US Forest Service and contract counties, as well as the state interoperability channels.

• The San Diego-Imperial County Regional Communications System (RCS) provides seamless, wireless communications for member local, tribal, state, and federal public safety/service agencies throughout San Diego and Imperial Counties. The RCS enables public safety and emergency response personnel to communicate more quickly and efficiently during an emergency by allowing communications both within and among different public safety/service personnel through the use the RCS or an existing compatible wireless communications system. CalTrans is an original partner and current participant in this system.

• The Los Angeles Regional Tactical Communications System (LARTCS) provides a fixed gateway infrastructure linking approximately 100 local, state, federal, and military agencies (in numerous radio bands) in the Los Angeles County area.

• The Sacramento Regional Radio Communications System (SRRCS) provides a consolidated communications infrastructure to approximately 45 law, fire, EMS, and public works users in the greater Sacramento area (including Yolo County). The CHP, CalTrans, California Exposition, and UC Davis Medical Center are participants.

• The CHP and CalTrans have constructed integrated Traffic Management Centers around the state to facilitate interagency collaboration, and in some case collaboration with local systems.

• Through the FIRESCOPE Program (**FI**refighting **RES**ources of **C**alifornia **O**rganized for **P**otential **E**mergencies), the California Fire Service has developed common operational protocols and frequency standards for integrated local-tribal-state-federal firefighting communications.

Current Status of Interoperability Technology

Much attention has been focused upon “black box” gateway technologies as the magic bullet for interoperability. As these local/regional programs and state system modernization takes place, there is an appropriate role for these bridging technologies. However, these tools are limited in use and should not be considered long-term fixes; they should be viewed as effective temporary links that create interoperable systems between disciplines or regions where they do not already occur, and are especially valuable in emergency response events. In 2004, the Department of Homeland Security (DHS) initiated a program known as RapidCom 9/30. It provided resources for the top 10 high-threat Urban Areas to achieve incident level interoperability. According to DHS, RapidCom engaged public safety officials to identify and incorporate each community’s key factors of frequency of use, standard operating procedures, regional governance, and training and exercises utilizing gateway technology. Work has already been done to duplicate this effort throughout the state of California, thus, creating incident level interoperability throughout the state.

Partner Organizations-Federal and State

At the federal level, two key partners are the Department of Homeland Security’s *SAFECOM* and *Interoperable Communications Technical Assistance Program (ICTAP)* programs. Both of these programs provide invaluable vision and leadership to the communications community.

- The *SAFECOM Program* provides research, development, testing and evaluation, guidance, and assistance for local, tribal, state, and federal public safety agencies working to improve public safety response through more effective and efficient interoperable wireless communications.
- The *Interoperable Communications Technical Assistance Program (ICTAP)* provides technical assistance on communications interoperability issues, primarily to Urban Area Security Initiative (UASI) cities, but can also provide services to other levels of government. Within California, ICTAP is working with a number of the state's UASI cities in the development of Tactical Interoperable Communications Plans (TICPs). The State has requested ICTAP's assistance in ensuring commonality between the various Urban Area TICPs and the State's communications interoperability efforts, to ensure a cohesive environment for our first responders.

At the state level, the *California Statewide Interoperability Executive Committee* (CALSIEC) was established in 2003 by OES in response to a FCC tasking for the management of designated interoperability spectrum. CALSIEC is made up of representatives of local, tribal, state, and federal first responder organizations within California and is working on the development of a comprehensive Statewide Communications Interoperability Plan consolidating all of California's current discipline-specific communications plans and establishing technical and operational protocols and governance structures for interoperability at all levels. CALSIEC has designated four geographic Planning Areas within California and has identified ten (10) aspects of the total interoperability picture (such as law enforcement requirements, EMS requirements, management of audio gateways, etc.) for a Working Group to address. More information on CALSIEC's membership and operating structure appears in on their website (http://www.calsiec.org/). It is important to note that in many instances the PSRSPC state agency membership also provides CALSIEC representation. As a result, there is a convergence at both the technical and communications planning levels between the two organizations. Indeed, CALSIEC is certainly viewed as a major partner and player in the state's modernization and interoperability efforts by addressing the statewide (local, tribal, state, and federal) needs.

SAFECOM Overview

Mission

The tragic events of 9/11 clarified the critical importance of effective emergency responder communication systems. The lack of emergency response interoperability is a long-standing, complex, and costly problem with many impediments to overcome. Interoperability is the ability of emergency response agencies to talk to one another via radio communication systems—to exchange voice and/or data with one another on demand, in real time, when needed and when authorized.

While several government programs have made great strides in addressing this issue, much of this work has been disconnected, fragmented, and often conflicting. In an effort to coordinate the various federal initiatives, the SAFECOM program was established by the Office of Management and Budget (OMB) and approved by the President's Management Council (PMC) as a high priority E-Gov initiative. More specifically, SAFECOM is a communications program within the Office for Interoperability and Compatibility (OIC) that provides research, development, testing and evaluation, guidance, tools, and templates on communications-related issues to local, tribal, state, and Federal emergency response agencies working to improve emergency response through more effective and efficient interoperable wireless communications.

SAFECOM is pursuing its mission on a variety of fronts and is consistently guided by the input of local and regional emergency response officials.

Governance

SAFECOM adheres to a bottom-up approach, which means the program relies heavily on local and state emergency response practitioners for input and guidance as it works to define and implement solutions for the interoperability challenge.

As a practitioner-driven program, SAFECOM has developed a governance structure that facilitates the input of local and state emergency response practitioners. Through the Program's Executive Committee (EC) and Emergency Response Council (ERC), the emergency response community and local, tribal, state, and Federal policy makers provide strategic input to the SAFECOM Program.

Initiatives

Rapid COM

On July 22, 2004, President Bush formally announced the RapidCom initiative, a program designed to ensure that a minimum level of emergency response interoperability would be in place in ten high-threat urban areas by September 30, 2004.

With the initial work of RapidCom now complete, incident commanders in each of the urban areas now have the ability to adequately communicate with each other and their respective command centers within one hour of an incident. With the input of local emergency response officials, RapidCom identified and advanced five "critical success factors" essential to interoperable systems as represented in the Interoperability Continuum.

Statewide Communications Interoperability Planning (SCIP) Methodology SAFECOM partnered with the Commonwealth of Virginia to develop a strategic plan for improving statewide interoperable communications with support from NIJ.

Based on the lessons learned from the Commonwealth of Virginia's planning process, SAFECOM released the Statewide Communications Interoperability Planning (SCIP) Methodology for integrating practitioner input into a successful statewide strategic plan. The SCIP Methodology serves as one approach for states to consider as they initiate statewide communications planning

efforts.

Statement of Requirements (SoR)
SAFECOM released the first-ever Statement of Requirements (SoR) for public safety communications interoperability in April 2004. This statement defines future requirements for crucial voice and data communications in day-to-day, task force, and mutual aid operations. The National Institute of Justice's CommTech Program (formerly AGILE) partnered with SAFECOM in formulating and releasing the requirements.

With the SoR, the nation's 60,000 emergency response agencies – for the first time – have a document that serves as a first step toward establishing base-level communications and interoperability standards for all emergency response agencies. The SoR helps the emergency response community convey a shared and vetted vision that ultimately will help private industry better align research and development efforts with critical interoperable communication needs.

SAFECOM Further Explained: Frequently Asked Questions of SAFECOM

Why can't emergency response agencies talk?

Inadequate and unreliable wireless communications have plagued emergency response organizations for decades. In many cases, agencies cannot fully perform mission critical duties because they are unable to communicate with other emergency response personnel who are responding to the same incident. These agencies are unable to share vital voice and/or data information via radio with other jurisdictions in day-to-day operations and in emergency response to large-scale incidents including acts of terrorism and natural disasters.

While mismatched technology accounts for part of the problem, it is only part of the story. As noted in a report published in February 2003 by the National Task Force on Interoperability, the emergency response community has identified the following as the key issues that hamper emergency response wireless communications today:

- Incompatible and aging communications equipment;
- Limited and fragmented budget cycles and funding;
- Limited and fragmented planning and coordination;
- Limited and fragmented radio spectrum;
- And limited equipment standards.

Why can't emergency responders use cell phones to talk to each other?

Unfortunately it's not that simple. Although emergency response practitioners regularly use cellular phones, personal digital assistants (PDAs), and other commercial wireless devices and services, these devices are currently not sufficiently suited for emergency response communications during critical incidents.

First and foremost, emergency response officials cannot depend upon commercial systems that can be overloaded and unavailable. Experience has shown such systems are often the most unreliable during critical incidents when public demand overwhelms the systems.

Emergency response officials have unique and demanding communications requirements. Optimal public safety radio communication systems require:

- Dedicated channels and priority access that is available at all times to handle unexpected emergencies;
- Reliable one-to-many broadcast capability, a feature not generally available in cellular systems;
- Highly reliable and redundant networks that are engineered and maintained to withstand natural disasters and other emergencies;
- The best possible coverage within a given geographic area, with a minimum of dead zones;
- And, unique equipment designed for quick response in emergency situations—dialing, waiting for call connection, and busy signals are unacceptable during critical events when seconds can mean the difference between life and death.

What is radio spectrum and why is it important to interoperability?

Radio spectrum is one of the nation's most valuable, finite resources. It is electronic real estate—the complete range of frequencies and channels that can be used for radio communications. Spectrum is the highway over which voice, data, and image communications travel. Inadequate radio spectrum is a major barrier to effective emergency response communications, both in major events and in day-to-day operations. Without access to effective radio spectrum, emergency

response personnel cannot communicate with their own agencies and with each other as needed.

What is P25?

Project 25 (P25) defines a suite of Technical standards for a digital wireless radio communications system that can be used by the emergency response community. While the FCC has mandated use of P25 standards on 700 Mhz Narrowband voice interoperability channels, its use on any other channel is voluntary. P25 enables multiple vendors to supply the products and services to the communications system users by defining eight interfaces for which standards are or will be developed. Each interface allows the products of one manufacturer to interoperate with products of other manufacturers by defining the signaling and messages that cross the interface. For example, an agency could purchase P25 portable radios from one or more vendors, mobile radios from other vendors, the base stations from others, and dispatch consoles from still other vendors; all would have the features the agency needs to accomplish its mission, and all would interoperate under the P25 standards. The P25 Steering committee is actively developing standards and protocols that emergency management/first responders will be using in the future.

What is the greatest obstacle in achieving seamless communications among the Nation's emergency responders?

Beyond the barriers discussed earlier, the greatest challenge is human. The challenge comes in helping stakeholders at all the levels of government understand the need for and the potential value of effective interoperability. More importantly, it requires giving all stakeholders a voice in the national process, understanding all stakeholder perspectives, and showing the advantages of participating in a coordinated effort. SAFECOM's approach is targeted at overcoming these barriers through the development of tools, templates, and methodologies in service of the emergency response community. The SAFECOM national strategy rests on the principle that every level of government involved in interoperability has a real voice in SAFECOM planning.

How does SAFECOM address the needs of emergency response agencies?

SAFECOM advocates a bottom-up approach which means the program relies heavily on local and state public safety practitioners input and guidance as it works to define and implement solutions for the interoperability challenge.

In promoting public safety communications interoperability, SAFECOM adheres to the following conditions and priorities:

- Local, tribal and state agencies will continue to own the vast majority of the public safety communications infrastructure;
- The priorities of local, tribal and State public safety communications systems are first and foremost to provide reliable agency-specific communications. Secondly, those systems should provide reliable local interagency communications. The requirement for reliable interagency communications between local, tribal, state, and Federal agencies is tertiary;
- The functional and technical requirements for public safety communications equipment vary across jurisdictions and disciplines and are determined at the local level;
- And, public safety communications will continue to operate on a variety of technologies across fragmented spectrum bands.

Based on those conditions, SAFECOM does not expect to promote a single solution to public safety interoperability across the nation. SAFECOM will support and promote a broad range of solutions with the following key elements:

- Technical and functional requirements should be defined at the local or tribal level up to the state and then to the Federal level;

- Solutions should involve a "system of systems" approach that incorporates existing technologies and allows for the development of new technologies and functionality in the future;
- And standards should be open to allow the interoperability of equipment from a variety of technologies and vendors.

How long will it take to achieve emergency response communications interoperability?

There is no quick and easy solution to solving communications interoperability issues. Achieving an optimal state of nationwide interoperability involves both human and technological factors and will be the result of a cumulative effort that involves coordination of processes and input from stakeholders across all levels of government.

Full interoperability could take 20 years because of equipment life cycles and time needed to develop and implement standards. In the mean time, SAFECOM and other organizations are working to ensure short-term solutions are in place.

What is SAFECOM doing to address interoperability in the short-term?

In the last year, SAFECOM has:

- Created the Federal Interagency Coordination Council (FICC) to coordinate funding, technical assistance, standards development, and regulations affecting communications and interoperability across the federal government;
- Published a Statement of Requirements which, for the first time, defines what it will take to achieve full interoperability and provides industry requirements against which to map their product capabilities;
- Issued a request for proposals for the development of a national interoperability baseline;
- Initiated an effort to accelerate the development of critical standards for interoperability;
- Created a Grant Guidance document that has been used by FEMA, COPS, and ODP state block grant program to promote interoperability improvement efforts.
- Established a task force with the Federal Communications Commission to consider spectrum and regulatory issues that can strengthen emergency response interoperability;
- Created a model methodology for developing statewide communications plans;
- Released a Request for Information to industry that netted more than 150 responses;
- And worked with the emergency response community (local, tribal, state, and federal) to develop a governance document that defines both how SAFECOM will operate and how participating agencies will work within that framework.

What is the Public Safety Statement of Requirements?

The SAFECOM Program developed the nation's first ever Statement of Requirements (SoR) for Wireless Public Safety Communications and Interoperability in coordination with the National Public Safety Telecommunications Council, the National Institute of Standards and Technology, and the Department of Justice's AGILE Program. This statement defines future communications requirements for crucial voice and data communications in day-to-day, task force, and mutual aid operations and serves as a first step toward establishing base-level communications and interoperability standards for all emergency response agencies. The SoR also helps the emergency response community convey a shared and vetted vision that ultimately will help industry better align research and development efforts with critical interoperable communication needs. In February 2006, SAFECOM released an updated version of the SoR with refinements based on input from the emergency response community.

ICTAP Overview

Interoperable Communications Technical Assistance Program (ICTAP)

G&T can provide true interoperable communications support for local and State first responder agencies through the provision of various types of technical assistance. As part of this mission, G&T administers the Interoperable Communications Technical Assistance Program (ICTAP).

ICTAP is a technical assistance program designed to enhance interoperable communications among local, State, and Federal emergency responders and public safety officials, and is associated with G&T's Urban Areas Security Initiative (UASI) grant program. The goal of the ICTAP program is to enable local public safety agencies to communicate as they prevent or respond to a WMD attack. ICTAP also leverages and works with other Federal, State, and local interoperability efforts whenever possible to enhance the overall capacity for agencies and individuals to communicate with one another.

ICTAP Further Explained: Frequently Asked Questions of ICTAP

What is ICTAP doing about regional interoperability?
DHS and ODP recognize that regional interoperability is the next challenge. Regional interoperable communications involve both intrastate and interstate collaboration. Because no one approach fits all cases, we encourage sites to coordinate with neighboring UASI regions, SAAs, and ODP on using grant funds for regional interoperable communications. ICTAP can help states and Urban Areas identify best practices and standards to enhance regional interoperability.

How do I request ICTAP assistance?

ODP provides technical assistance without charge to eligible states and local jurisdictions.

All TA requests must originate from the UASI or state grantee and should be coordinated through the State Administrative Agency (SAA). SAAs will submit TA requests either to the ODP Preparedness Officer assigned to their state or through the ODP Helpline. TA requests also can be submitted to ODP in writing (via regular mail or email) or by telephone (followed by a written request).

Each request for TA should include a brief description of:

1. The nature and extent of the requestor's homeland security issue
2. The type of technical assistance needed
3. The relevant strategic goal and objective in the state or urban area homeland security strategy
4. The efforts taken to address the need and the identification of other jurisdictions or agencies in the region that have similar needs
5. Plans for maintaining and sustaining efforts
6. The requestor's desired TA schedule
7. The UAWG POC

Can ICTAP provide examples of memos of agreement/understanding that newer sites can use as examples and templates for governance?
Yes. ICTAP will do so with the permission and concurrence of its state and local partners. Please contact your ICTAP Site Manager about your particular need. ICTAP can also provide examples of “sanitized” TICPs. These materials are available through your Site Manager and are being distributed to ICTAP points of contact at the UASI sites.

UASI locations are experiencing shortfalls in experienced staff to do planning work. What can ICTAP do to help?
In addition to ICTAP’s offering sites “no cost” assistance in technical, operations, and governance areas, sites are reminded that UASI and state grants may be used to hire staff and consultants. In addition, some sites and states are retaining the part-time services of recently retired employees who are subject matter experts with regard to local/regional communications systems. Sites should contact their State Administrative Agency (SAA)

or ODP Preparedness Officer about the specific provisions of the FY2005 Homeland Security Grant legislation.
Sites also should remember to check state and local laws and regulations regarding employment and consulting before using Homeland Security grant funding for this purpose.

.

TICP Overview

Tactical Interoperable Communications Plan Guidance

Tactical interoperable communications is defined as the rapid provision of on-scene, incident based mission critical voice communications among all first-responder agencies (EMS, fire and law enforcement), as appropriate for the incident, and in support of an incident command system as defined in the National Incident Management System (NIMS) model. The italicized below shows many aspects of tactical interoperable communications that should be incorporated into the development of a Tactical Interoperable Communications Plan. The Tactical Interoperable Communications Plan template is divided into six sections, most of which coincide with the elements of the Interoperability Continuum. The coinciding elements are noted in parentheses for your reference:

1. Urban Area Information

2. Governance Structure (Governance)

3. Interoperability Equipment (Technology)

4. Policies and Procedures for Interoperable Equipment (Standard Operating Procedures)

5. Incident Plan for Tactical Communications

6. NIMS Communications Unit Leader Training (Training and Exercises) Information on each of these sections, as well as recommended steps to take in developing each component of the plan are detailed in the following sections.

> *Tactical interoperable communications may be provided through the use of common equipment (common channels, cached radios or shared systems) or a gateway between dissimilar systems and/or radio frequency bands;*
>
> *Tactical interoperable communications may use fixed and/or mobile/portable solution(s).*
>
> *Tactical interoperable communications must be rapidly deployable at any time (24/7)*
>
> *Tactical interoperable communications should be fully operational within an hour of an incident occurring.*
>
> *Tactical interoperable communications requires oversight by trained Communications Unit Leaders, as defined within the NIMS, to support equipment deployment.*
>
> *Tactical interoperable communications plans should always be in support of long-term interoperability by building upon or accelerating long-term strategies and efforts.*

TICPs Further Explained: Frequently Asked Questions of TICPs

What is the purpose of the Tactical Interoperable Communications Plan (TICP)?
TICP serves as a planning tool to help sites exercise interoperable communications and to meet the Congressional mandate that grant recipients develop a tactical plan. TICP meets the requirements of Homeland Security Presidential Directive-5, *Management of Domestic Incidents*, and the DHS *National Incident Management System (NIMS)*.

How can ODP help us with the TICP?
Through its **Interoperable Communications Technical Assistance Program (ICTAP),** ODP will provide to any site or state, on a first-come, first-served basis, no-cost technical assistance in developing and exercising a Tactical Interoperable Communications Plan. ICTAP has assigned a site manager and a site technical lead to each UASI grantee and to states without a designated urban area. These individuals (and support staff) are available on a first-come, first-served basis to meet with a site's governance, operations, and technical working groups to facilitate TICP development and documentation and to support table top exercises.
The process for requesting ICTAP assistance is detailed in Question 19 below. Sites and states are encouraged to contact their ODP Preparedness Officer with questions.

How will ODP evaluate a Tactical Interoperable Communications Plan (TICP)?
There is no "pass" or "fail" for a TICP. ODP Preparedness Officers and subject matter expert staff will review and evaluate each TICP on its own merits. ODP recognizes that interoperable communications requirements will vary according to the specific needs of each site or state.

Does the TICP replace our strategic, long-term plan?
Not at all. The TICP should be developed in coordination with the long-term plan. The TICP is designed to prepare agencies for tactical interoperable communications during incidents. It should provide a snapshot of what radio equipment and methods your site currently has available and how those would be used in a tactical situation, such as the planned IED scenario.

What agencies should be included in the Plan? Should federal and state responders be included?

At a minimum, sites should include in the TICP all agencies that are represented in their Urban Area Working Group (UAWG), if applicable. Sites also should consider the role federal, state, and additional local agencies play in incident tactical response and include them in the Plan as appropriate. However, there is no requirement that non-UAWG agencies be included in the TICP.

What disciplines should be represented in the Plan?

At a minimum, law enforcement, fire, and EMS should be represented in the Plan. Sites should develop the Incident Communications Plan portion of the planned IED incident response validation in Section 5 of the TICP.

Do all UAWG agencies need to demonstrate communications interoperability in the IED scenario?
While the overall TICP should include all of the jurisdictions represented in the Urban Area, the Incident Communications Plan (Section 5 of the TICP) for the IED should only include agencies that would respond to the incident.

We are purchasing communications equipment with 05 funds. Should our Plan include these assets?

The TICP is designed to help jurisdictions identify the communications assets that they currently have and to develop operations policies for the use of that equipment during an incident. Only equipment that is expected to be in operational use by the October 1, 2005 planning deadline should be included in the TICP. **The TICP is competing for our**

UASI site's time and resources. May we use the same resources across different working groups? May we use plans already in place or underway to meet the TICP requirements to exercise the NIMS scenario?
Yes and yes. ICTAP encourages sites to use personnel across the different working groups, particularly where experienced staff are in short supply. ICTAP also encourages sites to adapt from current or proposed plans that meet the spirit and intent of the NIMS scenario. Please discuss using such plans and exercises already underway or planned within the next 12 months with your ODP Preparedness Officer.

We already have a communications plan. Do we need to re-do it in the TICP template?

If your site currently has a plan that includes the required TICP components (governance, equipment inventory, equipment policies and procedures, and training), you do not need to recreate the plan. However, all sites must develop the Incident Communications Plan (Section 5 of the TICP template) to support the IED scenario. If you are unsure whether your current plan complies with the TICP requirements, ICTAP can review the plan.

How do we get NIMS Communications Unit Leader Training?

The NIMS Integration Center is currently developing a training methodology and certification requirements for the Communications Unit Leader position. Once this is completed, ODP will provide the information to all sites developing TICPs.

What about a lack of continuity in governance working groups when key appointed and elected officials do not continue with the group?
ICTAP recognizes that many jurisdictions experience this situation. We have found that establishing a permanent core membership within a UAWG's interoperable communications organization, and delegating certain authorities and approvals in writing, can reduce the impact of such circumstances. ICTAP Site Managers can provide examples of lessons learned and best practices to help sites meet this challenge.

Gateways Explained

Sponsored by:

Communications Interoperability
with Capt. Eddie Reyes

Gateways — the good, the bad and the ugly — *Sponsored by Cisco Systems*

By Capt. Eddie Reyes

Last month I mentioned the word "gateways" but did not really elaborate. I am sure some of you asked "What exactly is a gateway?" Well I am glad you asked because for the next few minutes I am probably going to tell you more about gateways than you would ever care to know. But for those who have a sincere interest in knowing a little more about this "tool," get ready to read about my experience as the manager of one of the most robust gateway portfolios in the Mid-Atlantic Region.

I mention the word "tool" because that is exactly what gateways are, a tool in the toolbox of communications assets. A gateway is nothing more than a "gizmo" or a "black box" that allows the operator to connect several different radios (anywhere from 2 to 36, higher in some cases) together and allow first responders to talk with each other.

Today's gateways have lots of functionality, such as being able to connect any device that produces an audio signal (voice) and pass that transmission (message) to any other device that is capable of receiving audio signals. Those audio devices include portable and mobile public safety radios, telephones (landline, cellular and satellite), the internet or a local area network (LAN), dispatch consoles, CB radios, family service radios, you get the hint.

When you consider all tools from a radio cache to standards-based radio systems, properly engineered gateways with trained operators are somewhere in the middle. They come in three distinct types:

1. **Portable** – This type of gateway can be carried in a vehicle (back seat / trunk) and quickly deployed by attaching portable radios to it on the scene, mostly for line of sight communications. The Fire and EMS service seem to like this gateway a lot.
2. **Mobile** – This type of gateway is normally installed (hard) in a command or communications vehicle, usually with mobile radios and fixed antennas on the roof. This type of gateway can achieve line of sight or repeated interoperable communications.
3. **Fixed** – This type is normally hard mounted in an emergency communications center or antenna site with console or mobile radios, fixed antennas and normally operates in repeated mode.

But I must warn you, depending on whom you talk to, some people hate gateways and others love them. That is why I decided to call this month's article – the Good, the Bad and the Ugly, because I will

share with you my years of experience working on multiple gateway solutions.

I have found that some work great (good), some can be difficult to set up, operate and maintain (bad) and some can wreck havoc on a public safety agency's radio system if not engineered properly or there is operator error (ugly). This is why some people hate them.

Keep in mind that most gateways are controlled by some computer component and they will normally do exactly what the operator tells them to do, so most bad experiences with gateways are the result of some human error. On the other hand, once properly set up, properly engineered and under the control of a trained operator, they can be a real life saver in the event of a major catastrophe requiring many first responders from multiple agencies who are using different radio systems. This is why some people love them. So let's get started.

What are some current barriers to public safety interoperability? In other words, why do we need gateways in the first place? Well, for starters, public safety has to deal with incompatible and inadequate spectrum allocations or frequencies. That is, because there is a very finite amount of radio frequencies available to be used in any geographical area by public safety (and most of it is), we do the best that we can by using frequencies that are licensed to us without causing interference to any other frequency user out there. Have you ever stopped to think just how many radio users are really out there? Lots! I mean everyone from delivery drivers, taxi cabs and tow truck drivers to construction companies. They all have some type of private two-way radio on similar frequencies as public safety. Not to mention the cellular telephone providers that operate on some frequencies right next to the public safety spectrum.

Another reason to consider a gateway is there are limitations associated with the geographic coverage of most radio systems and today's public safety leaders want to be able to talk whenever they have to, from wherever they are, using whatever type of device is in front of them. With traditional radio systems, usually you had to be within the coverage area of your agency's radio system and have access to one of your agency's radios if you wanted to listen or talk to someone on the other end. Today's gateways have made this a thing of the past. With today's gateways, it's possible for example, for a chief of police on vacation in the mountains to talk with an incident commander on the perimeter of a hostage barricade situation involving the city manager when a cell phone is not one of the options available. In this scenario, if the chief has access to a secure computer with the proper software and hardware, he would be using radio over the Internet or Voice over Internet Protocol (ROIP). Literally, the sky is the limit today when it comes to public safety communications.

Finally, the most common barrier to public safety interoperability is not technical at all. It is the geo-political issues (politics and personal fiefdoms). There is a very common saying in the interoperability world that says: "Interoperability is 15% technical and 85% political" and it is true. Plain and simple, the real reason why some agencies still cannot talk with each other today is because egos and professional hatred have caused some department heads to decide they are not going to talk with each other even if technology allows it. I have been in meetings where a member of one law enforcement agency said no one should have the frequencies to his agency's radio system, even though it is public information.

Some clear advantages include:

- Can be implemented without significant radio infrastructure modifications
- Capable of interconnecting multiple HF, VHF low band, VHF high band, UHF, 800 MHz 900 MHz radios
- Can include trunked talk-groups, encrypted networks, cell phones, satellite phones, and the public telephone network. The danger with encrypted interoperable connections is that it is possible for the gateway to pass the encrypted radio transmission to a radio that is connected to the gateway which is not encryption capable. Again, this would be caused by human error because the gateway is simply doing what the operator prompted it to do.

Like with any other technical or tactical equipment that your agency uses, operation of the gateway

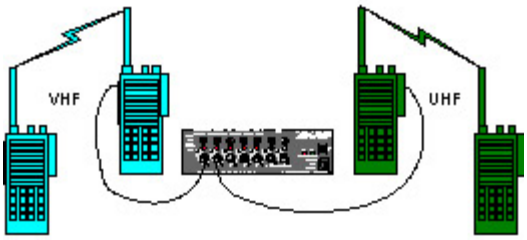
during non-emergency conditions requires:

- **Regular maintenance.** This is not as extensive as you may think. These devices are real work horses. They can be difficult to set up, but once they're up and running properly, they require very little maintenance. The fixed gateway at my agency has been running continuously since 1999 with no major maintenance and continuous service. The most important feature to remember with the maintenance of mobile or fixed gateways is making sure the radio programming is maintained current. Often times an agency with a radio on a gateway will change frequencies or talk groups. When this occurs, the radio has to be upgraded to reflect this change.
- **Routine testing with multiple agencies.** It is much easier to accomplish with fixed gateways because all you have to do is sit in front of a work station and test a quick radio connection with another agency. Of course governance should be in place which dictates how and when training is conducted. Once a month is recommended for fixed gateways. At least biannually with the portable and mobile gateways if not used more often during real events. Documentation is vital for liability purposes.
- **Readiness training.** Spend the time and money to receive formal manufacturer training. Most training is anywhere from 8 to 24 hours and no one knows the equipment better than the manufacturer. With time, each agency will develop "power users" and these folks can then become the agency's trainer if funds are limited.

Some gateway issues to be aware of include:

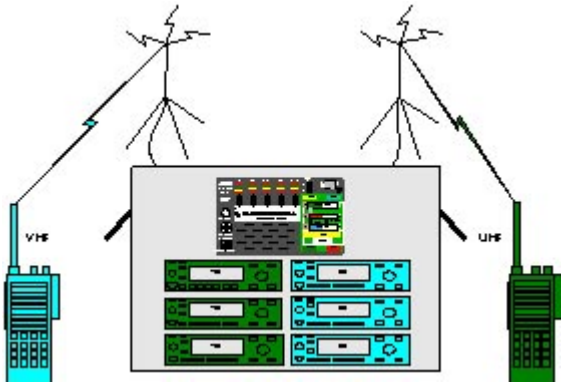
- **Licensing for radios associated with gateway operations.** The Federal Communications Commission (FCC) issues licenses for radios to be used in defined areas and gateways can consist of radios that operate outside of the licensed boundary but still remain within the region. While this is not a very serious issue because generally when these devices are used, it is for bonafide emergencies and the FCC has established regulations allowing the use of these radios outside of their licensed boundary during this condition. Yet, inadvertent connections or routine testing of these devices have caused formal groups, like the National Institute of Justice to have formal communication with the FCC to discuss this issue.
- **Inadvertent operations.** This occurs when an agency or operator is unaware that they have unintentionally connected a radio belonging to another agency which can cause the affected agency to lose its radio system, or a part of it for some time, until the error is located. In my region, several times, an agency's gateway inadvertently connected two radio systems together which caused the affected agency to lose one of its primary operating channels for three days until the problem could be located. Governance will play a huge role in ensuring that these incidents never occur. It is very important that everyone in a region know exactly who has which device and who to contact in the event of an inadvertent incident.
- **Un-coordinated operation (multiple links).** This occurs when too many gateways show up at the scene and everyone fires theirs up simultaneously. Again, regional governance will play a huge role in ensuring this doesn't occur. This is why it is vital to have effective human interaction ahead of time so when these devices start showing up, most communications unit leaders know each other and a thorough understanding occurs before any of the gateways are powered up. With the implementation of the National Incident Management System (NIMS), more and more each day, the formal recognition being given to the communications component will all but eliminate this potential. But nevertheless, you should be aware of it.
- **Channel Loading.** The gateway approach often requires a dedicated frequency (channel) for each of the interconnected radio systems throughout the duration of an incident. As a result proper planning is a must.

Portable Gateways:



Used on a temporary basis to link two or more radios to create two or more separate radio conversations. For example, the agency using the VHF radios on the left would give up one radio to attach to the gateway while the other agency using the UHF radios on the right would also give up one radio to attach to the gateway. Now all the responding units on these two radio systems would be able to talk with each other. You can keep adding radios up to the gateway's capacity. As I stated earlier, this configuration is a favorite of most fire and rescue departments because generally, they work a defined area, have a hard time reaching repeater sites from their portable radios inside blazing buildings and are quick and easy to set up. Using one of these configurations and the example cited above, two different fire companies could enter a building, using their own radios and talk with the incident commander. The real challenge with portable gateways is keeping the gateway powered and a charged battery on the portable radios attached to the gateway; this is why they are "temporary". But most portable gateways can be powered by a 12 volt car battery, standard batteries such as AA or 120 volt electricity. And as long as you keep the batteries charged, the connection will remain intact. Obviously if the gateway loses power, all radios attached lose interoperability and if a portable radio loses power, that agency loses interoperability capability.

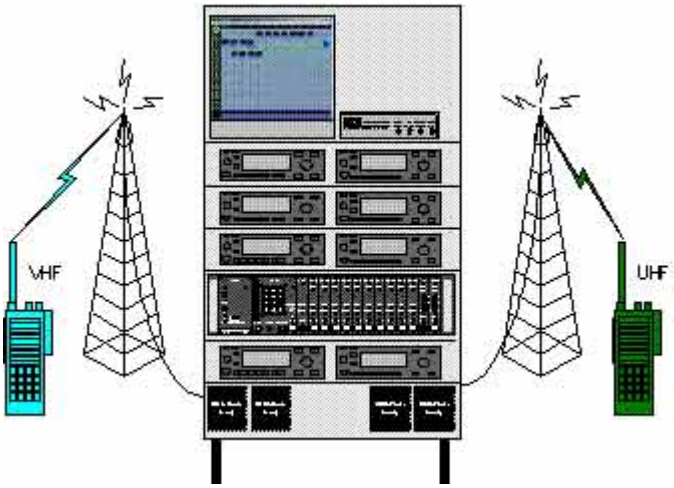
Mobile Gateways:



While mobile gateways can also be used on a temporary basis to link two more radios to create two or more separate radio conversations, generally, these mobile gateways are more robust using mobile radios instead of portables, which can generally communicate with repeater sites with no problems. This type of configuration is generally hard mounted in a communications or command vehicle and as long as the vehicle has power, the gateway will have power. Antenna placement on the roof of the vehicle is always a challenge because radios will cause interference to each other when placed that close to each other. So it is highly recommended that a professional radio company engineer the antenna placement. The beauty of this configuration is once all the radio systems of agencies in your region are programmed into the mobile radios (VHF, UHF and 800 MHz); a trained operator can have many agencies talking quickly and seamlessly. But again, this requires lots of human interaction and cooperation. In addition to being in communications and command vehicles, some agencies have chosen to mount this equipment in a trailer so that if the vehicle fails, it can be towed by another. Sometimes all you need is additional communications capability and not the entire command vehicle, so a trailer has a good application there. If the vehicle has satellite and/or network capability, this type of gateway can allow you to broadcast the radio traffic at the scene back to any other location on the

same network.

Fixed Gateways:



The most robust of all gateway configurations. It can be used on either a permanent or a temporary basis to provide real-time on demand communication and interoperability. This configuration is usually installed in or near a 24x7 emergency communications center where it is always available to trained, on-duty personnel who can create an emergency connection between two or more radio systems instantly. These gateways will generally require a professional engineer because you will be dealing with lots of antenna placements on a tower or roofline, to include lightning suppressors. In the event you use mobile radios for interoperability on the rack (generally 19") there will be lots of power conversion from 120 volts to 12 volts in order to power these radios and a robust power inverter/power supply will be necessary, The real beauty with this configuration is it can be controlled from virtually anywhere using a personal computer. This type of configuration gives an agency so much interoperability potential, such as radio over IP which allows you to securely route your public safety communications system to any PC with the proper settings which can be located virtually anywhere on earth. It will allow you to create 2 to 20 (even more in some cases) different connections, that is, allow up to 20 separate conversations without interference to each other.

This can be important during major events where each component wants its own talk path – command, fire suppression, special weapons and tactics, inner and outer perimeter, etc. Finally, it allows for a dispatcher to dispatch to multiple units from multiple agencies without the units having to be connected to each other.

In closing, I hope I have given you a better understanding on the public safety communications gateway. Like I stated earlier, it can be a real asset to your communications arsenal if it is set up right and due diligence is given to training. But a poorly engineered gateway at the hands of person with no training can be a real disaster to public safety communications. Gateways are manufactured by many of the public safety communications vendors and vary in size from two radios in a backpack to many radios in a computer room. Other parts of the country, which have great success using these devices, include Los Angeles County, CA; Hawaii; Florida; Houston, TX and Danville, VA.

If you are serious about considering a gateway for your application, please remember the three R's:

- **Regular maintenance.**
- **Routine testing with multiple agencies.**
- **Readiness training.**

PSRSPC Overview

The Public Safety Radio Strategic Planning Committee (PSRSPC) was established by the Public Safety Communications Act of 2002 (Government Code section 8592 et seq.). It continues an ad hoc effort underway since 1994 to develop and implement an integrated statewide Public Safety communications system that facilitates interoperability among the member state agencies, and fosters shared use and interoperability with local and federal public safety agencies. The following state agencies are members of the PSRSPC:

- The California Highway Patrol
- The Department of Corrections and Rehabilitation
- The Department of Fish and Game
- The Department of Forestry and Fire Protection
- The Department of General Services
- The Department of Justice
- The Department of Parks and Recreation
- The Department of Transportation
- The Department of Water Resources
- The Emergency Medical Services Authority
- The Governor's Office of Emergency Services
- The Governor's Office of Homeland Security

In order to achieve the objectives of the Public Safety Communications Act of 2002, the Committee has gathered information on existing public safety communications related collaborative efforts around the state, and has heard from several local and regional programs and from professional organizations representing public safety interests. The Committee will be reviewing and updating previous work efforts in this area, and will be developing a process for forward migration to meet the needs of California's public safety agencies.

The PSRSPC Work Effort

To accomplish the tasks assigned by the Legislature, the PSRSPC (consisting of the member agency Executives) has established the PSRSPC-TWG. It is comprised of technical staff within the PSRSPC member agencies. It is envisioned that the PSRSPC will create additional Working Groups as required to address various aspects of the effort. The PSRSPC-TWG has invited staff from the Military Department and the California Department of Health Services (CDHS) to participate in its work efforts. In order to communicate with the PSRSPC’s stakeholders and interested parties, a web site has been created. Under future work efforts, the PSRSPC will review proposals for communications equipment involving state funds to ensure that they promote interoperability and are consistent with this plan.

CALSIEC Overview

The California Statewide Interoperability Executive Committee (CALSIEC) has been tasked with managing the state and federally designated interoperability spectrum on behalf of all of our public safety first responders.

CALSIEC develops and maintains the agreements that define practices for the use of interoperability channels. It functions as part of the Standardized Emergency Management System (SEMS) / National Incident Management System (NIMS). CALSIEC was established and operates under a Federal Communications Commission charter to the states to administer that portion of the 700 MHz band designated as interoperability spectrum. California had an existing structure in the Governor's Office of Emergency Services to administer other existing state and federally designated interoperability spectrum, within the context of the Master Mutual Aid system. Building on the existing structure, the Director of OES chartered CALSIEC, in 2003, to combine existing efforts and to provide a single committee to adminiter all interoperability spectrums in California.

CALSIEC's structure follows the model recommended by the FCC. The recommendations recognized California's then-existing methods of administering the state's Mutual Aid channels, such as the California Law Enforcement Mutual Aid Radio System (CLEMARS) Executive Committee, as examples of successful collaborations of local, state, and federal agency representation.

Through subcommittees and working groups, CALSIEC (pronounced "cal-seek") will be developing a consolidated ***Statewide Communications Interoperability Plan***, incorporating California's traditional mutual aid channels with the new interoperability channels; and addressing the changes in protocols required to adapt to today's operational realities following the September 11, 2001 terrorist attacks.

A Potential Executive Committee and Subcommittee Template for Northern, Capitol/Bay Area, and Central CALSIEC Planning Areas

The Southern Planning Area instituted their Executive Committee Representation (which comprises the voting members) as follows:

The goal is to ensure that there is a good cross section of representation between law enforcement, fire, and the "general government" type agencies.

As a result, the Southern Planning Area Executive Committee is comprised of the following representatives:

- Three from each of the twelve Southern Planning Area counties
- Two from federal agencies
- Two from tribal organizations
- One from the military
- One from the CHP
- One from CDF
- One from EMSA
- One from CalSIEC
- Committee Vice Chair
- Committee Chair

Relative to the Southern Planning Area counties, it was presupposed that the "gang of five" would select their representatives. The "gang of five" is comprised of the following County representatives:

- Sheriff
- Senior Fire Official
- Health Officer
- A municipal Fire Chief
- A municipal Police Chief

The Southern Planning Area has established two Subcommittee Working Groups as follows:

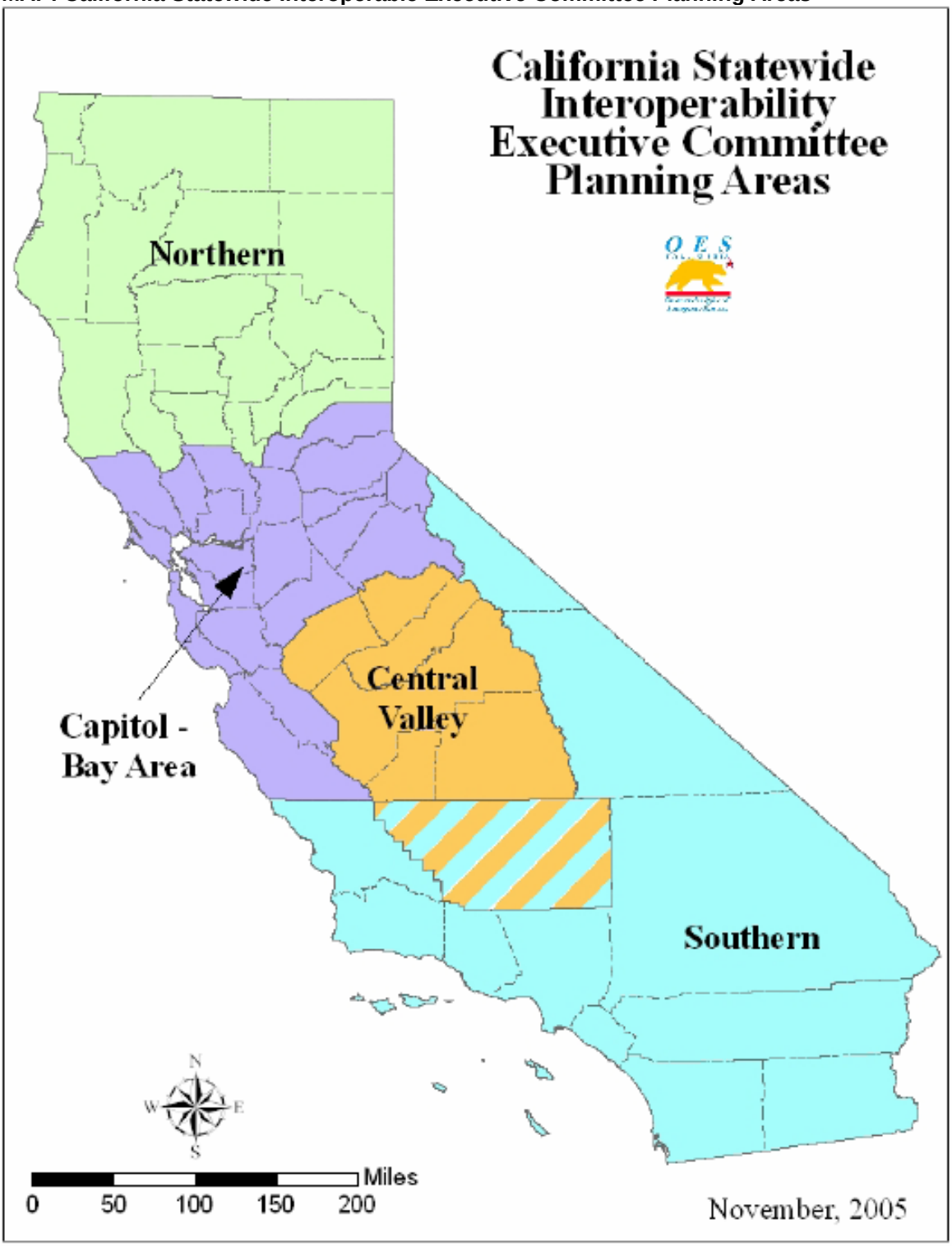
- Technical
- Operational

TABLE: Counties by CalSIEC Planning Area

CalSIEC Planning Areas				
	Northern	**Capitol/Bay Area**	**Central**	**Southern**
1	o Butte	o Amador	o Fresno	o Imperial
2	o Colusa	o Alameda	o Kern*	o Inyo
3	o Del Norte	o Alpine	o Kings	o Kern*
4	o Glenn	o Calaveras	o Madera	o Los Angeles
5	o Humboldt	o Contra Costa	o Mariposa	o Mono
6	o Lake	o El Dorado	o Merced	o Orange
7	o Lassen	o Marin	o Tulare	o Riverside
8	o Mendocino	o Monterey		o San Bernardino
9	o Modoc	o Napa		o San Diego
10	o Nevada	o Placer		o San Luis Obispo
11	o Plumas	o Sacramento		o Santa Barbara
12	o Shasta	o San Benito		o Ventura
13	o Sierra	o San Francisco		
14	o Siskiyou	o San Joaquin		
15	o Sutter	o San Mateo		
16	o Tehama	o Santa Clara		
17	o Trinity	o Santa Cruz		
18	o Yuba	o Solano		
19		o Sonoma		
20		o Stanislaus		
21		o Tuolumne		
22		o Yolo		

*Kern County participates in both the Central and Southern Planning Areas

MAP: California Statewide Interoperable Executive Committee Planning Areas



(Kern County participates in both Planning Areas)

MAP: OES Administrative Regions with Mutual Aid Regions

The $1million Question:

Within California, why do we need to have to separate interoperability committees, California Statewide Interoperability Executive Committee (CALSIEC) and Public Safety Radio Strategic Planning Committee (PSRSPC)?

While it may seem that the two groups are somewhat redundant, each has been established in response to a separate mandate. Each committee addresses different aspects of the overall public safety communications picture.

The PSRSPC was established and operates under a Legislative charter (in state law) as a state government committee to address the issue of state agency public safety communications system modernization, and to promote interoperability.

CALSIEC develops and maintains the agreements that define practices for the use of interoperability channels. It functions as part of the Standardized Emergency Management System (SEMS) / National Incident Management System (NIMS). CALSIEC was established and operates under a Federal Communications Commission charter to the states to administer that portion of the 700 MHz band designated as interoperability spectrum. California already had an existing structure in OES to administer other existing state and federally designated interoperability spectrum within the context of the Master Mutual Aid system. Building on that structure, the Director of OES chartered CALSIEC in 2003 to combine existing efforts and to provide a single body to administer all interoperability spectrum in California.

CALSIEC's structure follows the model recommended by the FCC. The recommendations recognized California's then-existing methods of administering the state's Mutual Aid channels, such as the California Law Enforcement Mutual Aid Radio System (CLEMARS) Executive Committee, and FIRESCOPE which deals with mutual aid, cooperative agreements, and fire/rescue regional policy issues are two examples of successful collaborations of local, state, and federal agency representation.

With OES acting as the common "host" to both of these committees, and with the Center for Collaborative Policy providing a common set of facilitators, there is "administrative reconciliation" to ensure that both groups are operating in a coordinated manner.