PART 3

WIRELESS COMMUNICATIONS ISSUES

This portion of the handbook is a brief description of frequency licensing and pertinent FCC Rules, a description of the newly reallocated television channel frequencies for public safety, a discussion of the FCC's "refarming" policy, a discussion of tower siting and FCC radiation specifications (OET Bulletin 65), information on various Federal initiatives, and a discussion of the issues surrounding interoperability.

Chapter 8

___

FCC Licensing, Rules, Regulations, and Related Issues

The FCC Rules and Regulations are printed in the Code of Federal Regulations (CFR), Title 47. Copies of the rules may be purchased from the Government Printing Office (GPO) (see resources in Appendix B). The following parts of CFR 47 are of interest for mobile radio communications services:

> Part 90 - Private Land Mobile Radio Services (PLMRS).
> Part 22 - Public Mobile Services.
> Part 24 - Personal Communications Services (PCS).
> Part 101 - Fixed Microwave Services.

Copies of the Rules may be downloaded from the FCC Web site (see resources in appendix B) or purchased at GPO bookstores.

Licensing

If you are buying a system or constructing it yourself, you will need to apply for a license. However, before applying to the FCC, you must obtain specific frequencies of operation from a frequency coordinator. The coordinator will check to see if any frequencies are available in your area and assist you in evaluating your options.

There are four coordinating bodies responsible for public safety-related frequencies:

> APCO - Association of Public-Safety Communications Officials.
> IMSA - International Municipal Signal Association.
> FCCA - Forestry Conservation Communication Association.
> AASHTO - American Association of State Highway Transportation Officials.

In the past, the coordinator for most local public safety frequencies has been APCO. However, with the implementation of refarming (see the end of this chapter), applicants may use the services of any frequency coordinator certified to coordinate frequencies in its pool of eligibility. Contact numbers for all four coordinating bodies are given in resources, appendix B.

The application form for radio licenses is FCC Form 601 for two-way radio frequencies. For FCC microwave frequencies, the application is FCC Form 415. Forms are available from the FCC or may be downloaded from its Web site.

In addition, if one of your base, repeater, or microwave stations requires a tower or an antenna tip with a height of 200 feet or more, you will need to complete a Federal Aviation Administration (FAA) Form 7460-1. If your antenna is within 5 miles of an airport runway and its height (in feet) is greater than or equal to 40 times the distance to the runway (in miles), you will also need to complete the same form.

If you are purchasing communications services from a licensed vendor, you will not have to obtain licensing. If you are sharing a system with another agency, make sure that the other agency is licensed. Normally, a letter contract or a memorandum of understanding (MOU) is drawn up between the licensed agency and a user.

FCC Rules and Regulations

Part 90

Part 90 covers the Rules for a number of *private land mobile radio services* including those for public safety. This section specifies the frequencies available for the various private and public safety services, licensing information, and technical and operating requirements. Technical rules include types of modulation, bandwidths, interference criteria, power output, and antenna height data.

Licenses require frequency coordination. Public safety agencies generally must use APCO for coordination. No Federal fees are required for license applications from local government applicants.

Docket 92-235. In FCC Docket 92-235, adopted in February 1997, the FCC reduced the number of service pools for frequencies below 512 MHz to two:

> 1. *Public safety,* consisting of local government, police, fire, highway maintenance, forestry conservation, emergency medical, and special emergency.

> 2. *Industrial/business,* consisting of power, petroleum, forest products, film and video production, relay press, special industrial, business, manufacturers, telephone maintenance, motor carrier, railroad, taxicab, and automobile emergency.

Certified frequency coordinators for the particular services are still required to assign frequencies for these services. The FCC also authorized centralized trunking at allocated frequencies from 150 to 512 MHz, providing no harmful interference is caused to existing channels.

Part 22

Part 22 of the Rules covers the licensing and technical requirements for *common carrier mobile radio services*, including paging and radio telephone services, rural radio telephone service, and cellular radio.

Public safety agencies may use these services as subscribers only; the licenses are held by the service providers.

Part 24

Part 24 covers the Rules for personal communications services. This unique set of Rules deals with the auctioning of frequencies in the 900 MHz and 2 GHz bands. There is little technical detail, since winners of the auctions may provide many different types of service within the areas where they have won licenses.

At this time, the majority of 2 GHz PCS licensees are providing cellular voice services similar to those in the cellular radio frequency band.

Part 101

Part 101 covers microwave point-to-point radio frequencies. Frequency coordination, licensing, and technical standards are identified.

Reframing

The "Part 90 reframing" was officially adopted by the FCC in several dockets:

> Docket 92-235 (6/15/1995).
> Docket 92-935 (12/23/1996).
> Docket 92-235 (2/20/1997).[8]

The purpose of this initiative is to reduce most of the bandwidths of Part 90 radio systems operating below 512 MHz, thus promoting an increased efficiency in use. The reduction is in two stages: first from 25/30 KHz to 12.5/15 KHz and then from 12.5/15 KHz to 6.25/7.5 KHz bandwidths over a period of time. Licensees will not be required to replace their equipment to meet the band reduction requirement.

Currently, manufacturers are required to supply new equipment meeting the 12.5/15 KHz bandwidth specification, allowing for a smooth changeover. The bandwidths must be halved by manufacturers again by January 1, 2005. More details regarding reframing may be found in the footnoted reference.

Frequency Reallocation

In July 1995 the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA) established the Public Safety Wireless Advisory Committee (PSWAC) to evaluate the wireless communications needs of federal, state, and local public safety agencies through the year 2010 and recommend possible solutions to identified problems. In the PSWAC final report, published in September 1996, five primary areas of concern were documented: operational requirements, technology

---

[8] Ericisson, *Reframing - Truths and Myths* (brochure), February 1998.

issues, technology transition, interoperability, and the need for additional spectrum. PSWAC recommended utilizing portions of the 746-806 MHz band (UHF TV channels 60-69).

When the FCC reallocated an additional 24 MHz of spectrum in the 700 MHz band for public safety use (specifically TV channels 63, 64, 68, and 69), the Public Safety National Coordination Committee was impaneled to establish plans for the use of the frequencies designated as interoperability channels. The net effect will be to double the amount of spectrum available for public safety communications (figure 8-1).[9]

The work of the NCC's Implementation Subcommittee identified the need for an information resource to support the planning and pre-coordination necessary for efficient and effective allocation of the 700 MHz public safety spectrum.

The National Public Safety Telecommunications Council (NPSTC), an ad hoc federation of federal, state and local associations and agencies, along with the Public Safety Communications Council (PSCC), an association of the four FCC certified public safety frequency coordinators, requested the development of a pre-coordination database designed to facilitate inter-regional coordination in the pre-allotment of frequencies, the development of state or regional plans, and the automation of initial and amended applications for frequency use.

Figure 8-1. Public Safety Spectrum Doubles

---
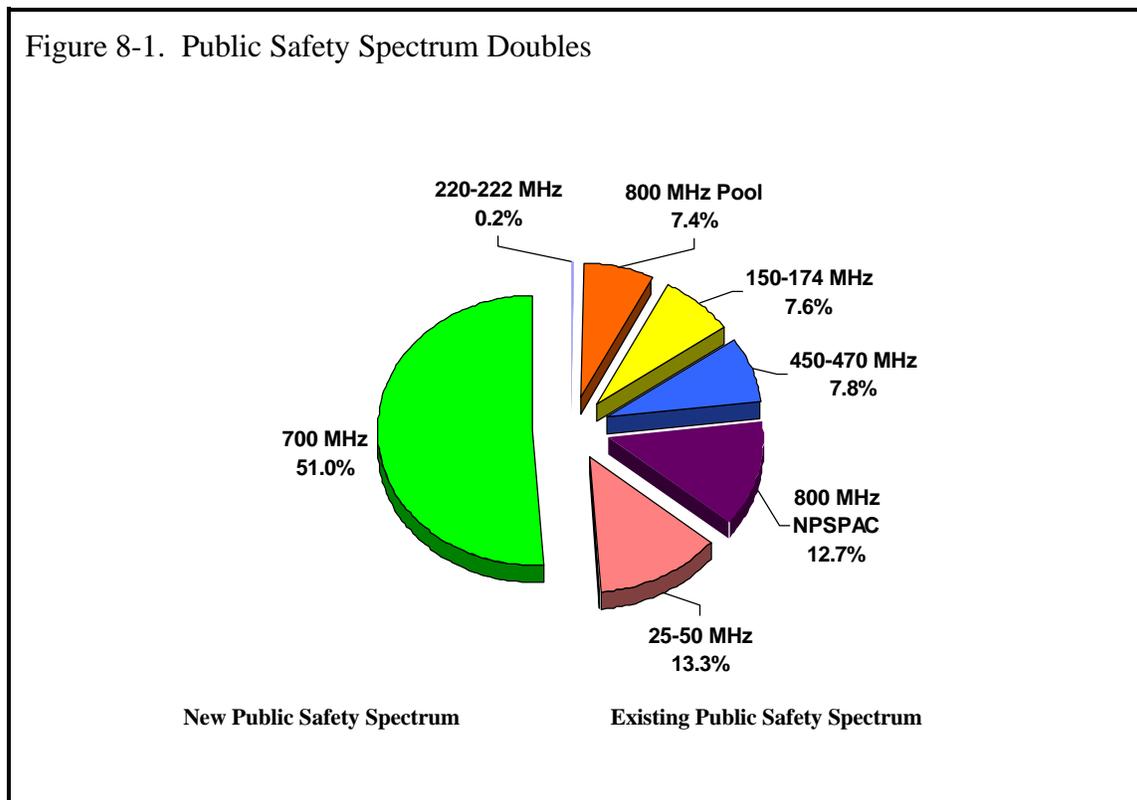
[9] "FCC Allocates More Spectrum to Public Safety," *Government Technology* (March 1998): 12.

Computer Assisted Pre-coordination Resource and Database (CAPRAD)

Originally envisioned as a notebook of available frequencies in the newly allocated 700 MHz public safety spectrum from which planners could formulate regional plans and select channels from for use within their regions, the Computer Assisted Pre-coordination Resource and Database (CAPRAD) has evolved into a suite of tools and resources which will assist regional planners, coordinators and users in managing the 700 MHz band from regional planning to consumer licensing.

The CAPRAD system features website access with a graphical user interface, an informational front page and secure access for registered users. The system is comprised of several interactive, relational databases which provide a frequency availability "notebook", search and report generating tools, interface to the PSCC's automated systems, and on-line help facilities, manuals and resources for planning, allotments and licensing applications (see figure 8-2). The system also serves as a repository for supplemental information such as completed regional and state plans, lists of broadcast television channels with potential impact, the final FCC report and order frequency table, contact information for RPC chairpersons and others as required, plus links to valuable sites and services available on-line.

Figure 8-2. Sample CAPRAD Screen

The CAPRAD system's state-of-the-art architecture, multi-level security protocols, and mirrored data management plan ensure both system integrity and system reliability. Fully integrated technical features of the hardware, software and support equipment provide exceptional system performance, availability, and security of information.

Years of planning by the NPSTC sponsored technical oversight working group, which included NPSTC technical membership, public safety frequency coordinator representatives and regional planners from across the country, and many months of development by the NPSTC Support Office and TEQ Services, Inc., a database and information systems firm in Englewood, Colorado, resulted in a database which will transform the regional planning process nation-wide.

Planning for and operation of the CAPRAD system is administered by the National Law Enforcement and Corrections Technology Center-Rocky Mountain Region, NPSTC Support Office. The NLECTC-RM is a program of the National Institute of Justice and is sponsored by the University of Denver through the Denver Research Institute (DRI). Special Federal funding supported the development of this database, as well as the outreach and training efforts required to assist the frequency coordinators and 55 regional planning committees (RPCs) in the use of the database and regional planning efforts.

4.9 GHz Band

Further FCC reallocations of the available spectrum occurred in February 2002. The 4.9 GHz band (4940-4990 MHz), originally transferred from Federal Government to private sector use in 2000 as substitute spectrum for the 4635-4685 MHz band which was reclaimed for Federal Government use, was reallocated to public safety use. This reallocation is now the largest ever to be made in the interest of public safety nationwide encompassing 50 MHz of spectrum.

Figure 8-3. Public Safety Radio Spectrum Bands With Newly Allocated 4.9 Ghz Band
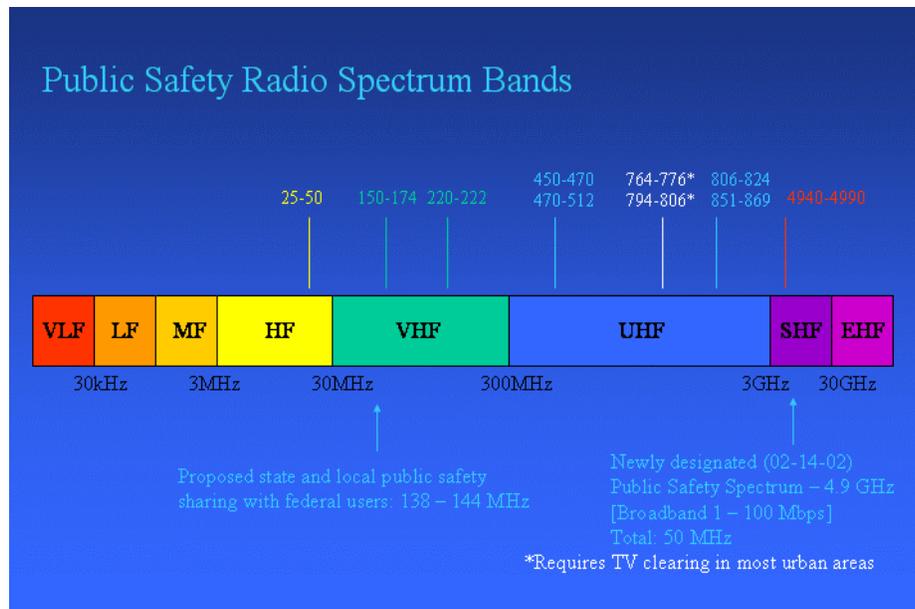
The 4.9 GHz band is designated for fixed and mobile wireless services use in support of public safety. The FCC's actions align with new national priorities focusing on homeland security and are intended to ensure that entities involved in the protection of life and property possess the communications resources needed to successfully carry out their mission. This allocation and designation will provide public safety users with additional spectrum to support new broadband applications such as high-speed digital technologies and wireless local area networks for incident scene management. The spectrum can also support dispatch operations and vehicular or personal communications.

Proceedings are underway which will establish the 4.9 GHz band licensing and service rules; define eligibility to use the band, including the scope of the public safety designation; delineate specific band segmentation and channeling plans; identify the interference impact on 4.9 GHz band operations from the adjacent U.S. Navy operations band; classify utilization of the band in a manner that will not interfere with the adjacent astronomy operations radio band; implement technical standards for both fixed and mobile operations on the band; and characterize innovative licensing approaches to serve public safety.

Chapter 9

Tower Siting and Radio Frequency Electromagnetic Radiation Exposure

Towers

All radio systems require towers to hold the antennas that transmit and receive radio energy. The higher the tower, the larger the coverage area for a given antenna. And, in general, as the capacity of radio systems is increased, more towers are required to attain necessary reliable area coverage.

Tower permits are issued by local zoning departments which require applicants to submit proposals for their approval. A portion of the local zoning ordinances is related to Federal requirements. These requirements include compliance with the National Environmental Policy Act (NEPA), the National Historic Preservation Act (NHPA), the Migratory Bird Treaty Act (MBTA), and the Endangered Species Act (ESA). Included in the NHPA are protections of certain Native American and Native Hawaiian tribal properties. Historic properties getting special treatment are those listed in the National Register, which is kept by the U.S. Department of Interior.

These acts are described in detail in the FCC Rules and Regulations, Sections 1.1301 through 1.1319. To meet the requirements of these acts, it may be necessary to complete an Environmental Assessment (EA) or an Environmental Impact Statement (EIS) to demonstrate tower installation compliance. There are other federal environmental requirements including meeting the FCC standards for hazardous radiation described below.

Although application processes vary from one governmental body to another, public hearings are usually required to receive input from those supporting or objecting to proposals. Unfortunately, the "not in my backyard syndrome" has been a powerful influence on the results of these hearings. The public often wants better public safety services but is not willing to accommodate new towers in their neighborhood without a battle.

Many local zoning ordinance policies are written to maximize the number of users on existing and new towers in order to minimize the total number of towers.   In addition, the ordinances are written to maximize the number of "stealth" towers where appropriate. Stealth towers take advantage of existing natural and man-made structures such as high building roofs, church steeples, mountain sites and imitation trees. Anything that can be done to make towers less aesthetically imposing helps with the approval

process. For example, monopoles are often less obtrusive then lattice towers. However, most antennas need to be high, and it is difficult to put up beautiful towers at a reasonable cost.

Fortunately, public safety agencies have a bit more clout than private entities. Where possible, negotiating with private applicants for antenna space is often beneficial for both the private and public entities. The Communications Act of 1996 contains language which requires communities to accommodate "reasonable tower heights," which is often useful in applying for tower permits. If permits are not approved, suing under the Act is possible but can take a very long time, so it is better to work carefully with and educate the public before and during the permit process.

Many tower leasing companies have space available for public safety organizations' antennas on an annual fee basis providing the new user does not cause interference to current users. Some of the larger tower companies are American Tower, SBA, Signal Tower, and Pinnacle Tower.

Towers near airports require special consideration. If a tower will be 200 feet or more high or is to be located within five miles from an airport runway (above a height slope of 40 feet per mile from a runway), a radio license applicant must also file a Federal Aviation Administration (FAA) Form 7260-1 with a copy to the FCC. The FCC will not issue a license without prior approval of the FAA.

When communications towers are constructed, the owner must register the antenna structure by filing FCC Form 854 either electronically or via paper. The registered tower is given a number and inventoried by the FCC. The criteria for FCC registration are identical to those of the FAA above.

# Radio Frequency Electromagnetic Radiation Exposure

All licenses and renewals filed after September 1, 2000, require that the applicant certify that the environmental regulations of Section 1.1307(b)(1) of the FCC Rules concerning RF exposure will be (or are being) met. The hazardous radiation calculations especially for multiple transmitters at a site can be complex and may require the services of a Registered Professional Engineer who practices in this area to perform the calculations.

(Note: The methodology for making calculations is outlined in the FCC Office of Engineering and Technology Bulletin #65, "*Evaluating Compliance with FCC Guidelines for Human Exposure to Radiofrequency Electromagnetic Fields*" upgraded in August, 1997, by a mandate from the 1996 Communications Act. The document may be downloaded at www.fcc.gov/oet/rfsafety.)

Before upgrading the bulletin in 1997, the FCC held extensive meetings with health and safety agencies, the medical community and universities working in RF non-ionized radiation research and confirmed there is no credible research showing any hazardous effects to human beings other than exceeding thermal dissipation rates within our bodies. This is analogous to a microwave oven where one places food into a known RF radiation field for a time period to heat it up. If you are exposed to RF radiation at too high a power and for too long, you will also "cook." Consequently, transmitter output powers may have to be reduced or transmitters be turned off while technicians work near transmitters or climb towers.

There are two standards listed in OET Bulletin #65, one for personnel who work on radio systems considered "occupational" and the other is the "general public". The standards vary with frequency bands because the human body is resonant and therefore can absorb more energy in the 30 to 300 MHz range than at other frequencies. Guidelines concerning fencing and signage where hazardous radiation may exist are also spelled out in the bulletin.

Figure 9-1 shows a graph of the standards for radiation densities. The worst frequency for RF absorption is in the 100 to 300 MHz range. At that frequency, the highest permissible RF level in controlled areas is 1 mW/cm^2 for 6 minutes of exposure time and 200μW/cm^2 in uncontrolled areas for 30 minutes of exposure time.

Figure 9-1. FCC Limits for Maximum Permissible Exposure (MPE)
Plane-wave Equivalent Power Density
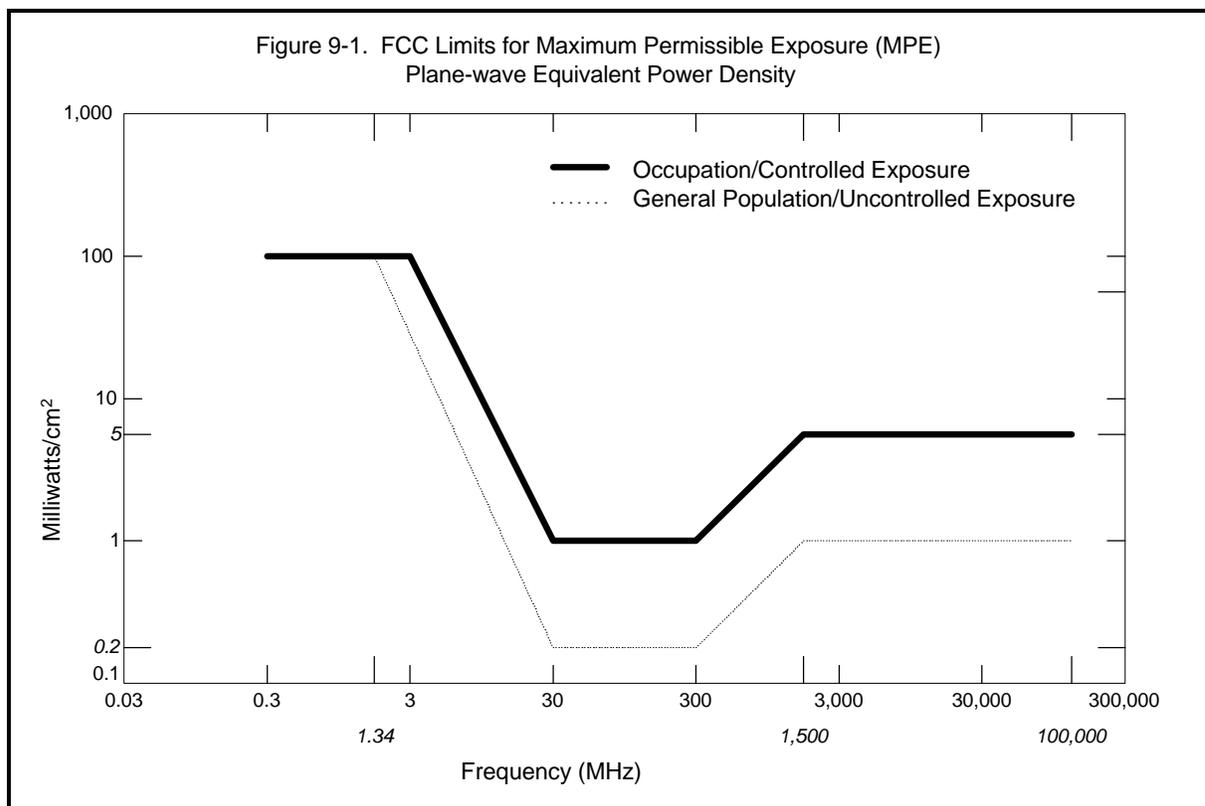
Chapter 10

_____

Federal Government and Other Initiatives

In addition to the FCC, the Federal government has a number of other initiatives that impact agencies at the State and local level. Some of the more obvious ones are discussed here.

NCIC 2000

The FBI's National Crime Information Center (NCIC) computer provides all 50 States with access to the records in the databases. Currently, more than half a million users in some 80,000 agencies make 1.7 million inquiries per day to NCIC.[10] Harris Corporation has been awarded a contract to upgrade the NCIC system, which includes replacement of the old computers with new IBM® 390 mainframes and operating systems. Projections call for up to 2 million transactions per day.

The NCIC 2000 project expects to support communication with mobile-imaging units in patrol cars.[11] The upgraded system will require that communicating units use TCP/IP over X.25 protocol before the system is placed online. After many users' requests, the FBI is considering other protocols such as TCP/IP over point-to-point protocol (PPP), Ethernet, and additional options. The FBI has conducted tests using various communications technologies, including CDPD, 800 MHz alone, and 800 MHz in conjunction with microwave.

An NCIC 2000 workstation has been developed for mobile-imaging units to transmit and receive mug shots and fingerprints. Plans call for high-quality imaging, including mug shot field imaging with high- quality field cameras so that officers may simply point and click. A quick check of a right index fingerprint will be possible with the fingerprint-matching subunit planned for use in the system. When the system is complete and operational, a field officer will be able to:

➡   Enter a wanted person's fingerprint, mug shot, and identifying images.
➡   Identify a wanted person using a fingerprint.
➡   Modify a fingerprint entered into NCIC 2000 with a new fingerprint.
➡   Link a wanted person's fingerprint to one entered by another organization.

_____

[10] "FBI Readies New Crime Information Network," *Government Technology Reseller* (March 1998): 30.

[11] Ibid.

➡   Cancel a wanted person's fingerprint.
➡   Receive ownership of a linked fingerprint when the original owner cancels the entry.

The NCIC workstation and the MIU (mobile imaging unit) are be based on Intel's Pentium technology. In addition, the FBI has published requirements for peripheral equipment (printers, scanners, data radio modems, etc.), commercial off-the-shelf software (COTS), and NCIC 2000 workstation applications software (to be provided by the FBI to the States at no cost). All of these specifications, as well as the latest status on the testing and implementation of the NCIC 2000 project, may be found by contacting the FBI directly (see resources in appendix B).

Public Safety Wireless Network (PSWN)

The Public Safety Wireless Network (PSWN) was created in 1996 through the National Partnership for Reinventing Government as an effort to re-engineer how government provides services to citizens through more effective use of information technology, among other approaches.

PSWN was specifically created as a jointly sponsored endeavor between the Department of Justice and Department of the Treasury to plan a nationwide wireless communications network for providing interoperability among federal, state, and local public safety entities. The Federal Law Enforcement Wireless Users Group (FLEWUG), which represents the interests of federal agencies with public safety missions, helped establish PSWN. In addition to oversight from the Departments of Justice and Treasury, the PSWN Program reports to the Government Information Technology Services Board (GITSB) .

The PSWN program is funded annually by the Departments of Justice and Treasury, with annual funding levels based on appropriations made by Congress. The program is a 10-year initiative.

Program Overview

The overall mission of the PSWN program has been to formulate a comprehensive plan for interoperability among wireless networks so local, state and federal public safety requirements can be met. PSWN is pursuing a number of system development support activities, analytical studies and outreach efforts which may be viewed on their website (see resources in Appendix B). The program is working to achieve a vision it shares with the public safety community -seamless, coordinated and integrated public safety communications for the safety and efficient protection of life and property. The program's primary objective is to develop a national implementation plan for interoperability based on an information and experience baseline developed during the course of the program.

The PSWN program is pursuing technical assistance, case studies, and analysis efforts throughout the country, including San Diego , the Mexican border area, Alaska, Arizona, Idaho, Mississippi, Tennessee, West Virginia, and Wyoming. Through these efforts, the program hopes to develop a better understanding of existing public safety interoperability problems. The field data is helping leaders understand public safety communications limitations because the information is comprehensive rather than anecdotal.

Near- and long- term recommendations for solutions to improve interoperability will be based on this analysis. These efforts have evolved into pilot projects sponsored by PSWN which are being used as test-beds for demonstrating interoperability technical, policy, and piloted solutions. In addition, the PSWN program participates in test-beds, demonstrations and special events sponsored by other organizations such as the National Institute of Justice (NIJ).

PSWN has completed an effort to develop a Wireless Interoperability National Strategy called Public Safety WINS. Public Safety WINS serves as the PSWN program's key mechanism to synthesize and apply the data the program has gathered into a coherent solution - oriented strategy for improving interoperability.

PSWN is also pursuing a number of directed and special studies in the areas of coordination/partnerships, funding, spectrum, and standards. The program is trying to help the public safety community better understand various aspects of spectrum policy, legislation, management and regulation through a number of reports that can be found on the PSWN website library.

The National Institute of Justice and Its Interoperability Program

Created by the Omnibus Crime Control Act of 1968, the National Institute of Justice (NIJ) is the research and development arm of the U.S. Department of Justice. With one of its primary mission elements aimed at developing new technologies to fight and improve criminal justice, NIJ (through its Office of Science and Technology (OST)) is addressing the issue of interoperability among criminal justice and other public safety agencies. The concept of interoperability is discussed further in Chapter 11 below.

Advanced Generation of Interoperability for Law Enforcement (AGILE) Program

The National Institute of Justice (NIJ) has developed a focused, comprehensive program to address interoperability - the Advanced Generation of Interoperability for Law Enforcement (AGILE) Program. The AGILE program was created in 1998 to pull together all of the interoperability projects currently underway at the National Institute of Justice. AGILE's strategy addresses both short- and long-term interoperability solutions involving wireless telecommunications and information technology applications through three program elements:

✦ Standards
✦ Research, Development, Testing, and Evaluation
✦ Outreach

Developing Interoperability Standards for Public Safety

NIJ is identifying, adopting, and when necessary, developing open architecture standards for voice, data, image, and video communications systems for the public safety community. It is doing this in partnership with NIJ's Office of Law Enforcement Standards (OLES), located within the National Institute of

Standards and Technology (NIST); the National Telecommunication and Information Administration (NTIA); and other key organizations. AGILE is also working with the Global Advisory Committee.

Integrating, Testing, and Evaluating Interoperability Technology

The AGILE program will use operational test beds to integrate, test, and evaluate technologies that can contribute to addressing interoperability needs. AGILE is developing new technology solutions when shortfalls of existing technologies are identified. Results of operational evaluations will be shared with State and local public safety agencies.

Raising Awareness of Interoperability

AGILE aims to raise the awareness of interoperability issues through an outreach program so that policy makers and public safety leaders can make informed and cost-effective decisions. Through technology assistance to State and local agencies, AGILE helps disseminate short-term interoperability solutions, lessons learned or best practices, and NIJ's standards for interoperability as they are established.

Up to date information on the AGILE program, as well as other developments in interoperability, can be found on the AGILE website (see Resources).

Mobile Broadband for Emergency and Safety Applications (MESA)

Project MESA is a collaborative partnership made up of the European Telecommunications Standards Institute (ETSI) and the Telecommunications Industry Association (TIA) in the United States to generate the specifications for a suite of wireless technologies requiring the mobile and fixed radio transmission of data rates of up to 2 MB per second for emergency services, law enforcement, medical services and civil defense entities. The activity of this partnership devoted to public safety is called the Public Safety Partnership Project (PSPP) which constitutes the legal and operational framework for the standards developments. Accomplishments may be checked out on the Project MESA website, www.projectmesa.org.

Specific aims of the group are to provide common European and U.S. standards for:

> * The communications management at crisis and disaster centers by public safety officials to minimize the loss of personnel and assets.

> * The delivery of fire information communicated by sensors attached to fire fighters in burning structures to the fire management team to optimize fire fighting activities. Also video and sensor communications from planes over forest fires to better aid the protection of fire fighters and maximize the use of fire equipment.

> * Front line medical assistance for injured citizens including the monitoring of vital medical signs, two-way communications of EMS technicians to a medical facility, and streamed video.

* Interconnection of broadband satellite constellations to ensure stable communications from remote areas where terrestrial infrastructures have been seized during natural disasters.

* Coordination of military requirements for a wide variety of applications. For example, with terrorist activities possible and the potential for small military conflicts, the standards could be applied to NATO or U.S. Army "commercial procurement of off-the-shelf (COTS)" equipment.

* Communications from mobile robotics used by public safety and the military to inspect and report video and audio information via wireless communications from inside dangerous territories. This includes the discovery of injured people in hazardous areas due to earthquakes or fires, narcotics undercover investigations, SWAT team actions, automated inspections in inaccessible regions etc. and military operations including the discovery of mine locations.

*Interoperability with existing and future broadband LEO and MEO communications satellites and High Altitude Platform Systems (HAPS). The Project MESA team believes satellite and HAPS communications will accomplish the interoperability out of small cell regions when necessary.

* Quickly establish "ad hoc" networking to deploy broadband communications integrated with terrestrial networks in both the public safety and military sectors.

Additional applications may include:

* Airport security by transmitting suspect identification for fast broadcast to the public safety staff.

* Remote evidence gathering by law enforcement and peacekeeping operations.

* Airplane or helicopter surveillance communications of video, audio and data.

* Mobile surveillance for transmission of camera video to public safety teams.

* Electronic news gathering for radio and TV stations.

The Project MESA specification will complement, in terms of bandwidth positioning, existing and planned narrow band and broadband wireless standards. The project genesis was due to the APCO activities in their pursuit of Project 34 and the ETSI DAWS (Digital Advanced Wireless Services) program. A resolution to support Project MESA by making new spectrum available is slated to be discussed at the 2003 World Radio Conference (WRC 2003).

Chapter 11

Interoperability

"Lack of radio interoperability" is usually highlighted as one of the major problems following any large-scale public safety event, be it a bombing such as Oklahoma City, a hostage incident such as Columbine, wildland fires, or hurricanes such as Andrew. The events of September 11 again underscored the need for improvements in our ability to talk to one another, a capability hampered for years by technical, operational and political barriers, and by a lack of funding to make needed changes. Too often, interoperability is the forgotten stepchild as systems are improved or replaced.

Three Types of Interoperability

Interoperability falls into one of three categories. The PSWAC Final Report provides the following general descriptions of each:

- Day-to-Day

    1. Commonly used in areas of concurrent jurisdiction

        a. Agencies need to monitor routine traffic
        b. Minimizes need for dispatcher-to-dispatcher interaction

    2. If agencies are on different bands, may involve multiple radios in each vehicle

        a. Difficult for personnel using portable radios

    3. Infrastructure based interoperability is not efficient due to continuous use of an extra RF channel by each participant on a different band or system

- Task Force

    1. Usually involves several layers of government (fed/state/local)

    2. Opportunity for prior planning usually is present

3. Generally involves use of portable and/or covert equipment

4. Often requires extensive close-range communications

5. Nature of traffic is such that wide area broadcast is usually undesirable

6. May rove in and out of infrastructure coverage (metro to rural, in and out of buildings, etc)

7. Often implemented by exchanging equipment

- Mutual Aid

  1. Can involve many agencies with little opportunity for prior detailed planning (e.g. riots or wild land fires)

  2. Often requires assignment of several to many small groups, each on it's own talk group or frequency (tactical communications)

  3. Once on-scene, generally involves use of portable radios

  4. Many incidents are in rural areas out of infrastructure range

A detailed study by the PSWAC Interoperability Subcommittee found that 95% of all interoperability requirements fall into the "day-to-day" category. Good local communications must be promoted first. As an example, "automatic aid" where the closest unit(s) to an incident respond, regardless of jurisdiction, has been embraced by the fire services for many years, and is starting to make its way into the law enforcement community. Local interoperability is a must for automatic aid to work. It is the first, largest, and most important piece of the interoperability puzzle.

> ☞ Did you know?
> "Interoperability is the ability to talk to who you need to talk to when you need to talk to them. It is not the ability to talk with everyone all of the time."
> -- Chief Harlin McEwen (Ret), Chair, IACP Communications & Technology Committee

Task Force interoperability is more regional in nature. Once agencies have local interoperability, their next priority for communications is with other public safety agencies in their region/state. This is the second, and mid-sized piece of the interoperability puzzle.

Finally, mutual aid, typified by the massive multi-agency, multi-state responses seen in New York City and at the Pentagon on September 11, and experienced across the country each year for earthquakes, wild land fires, floods, hurricanes and other large-scale events, is the third type of interoperability. This is the national component of the interoperability puzzle. Mutual aid is usually tied to compacts implemented by state statute, thus the states must play an important role in interoperability as it expands to their boarders and beyond.
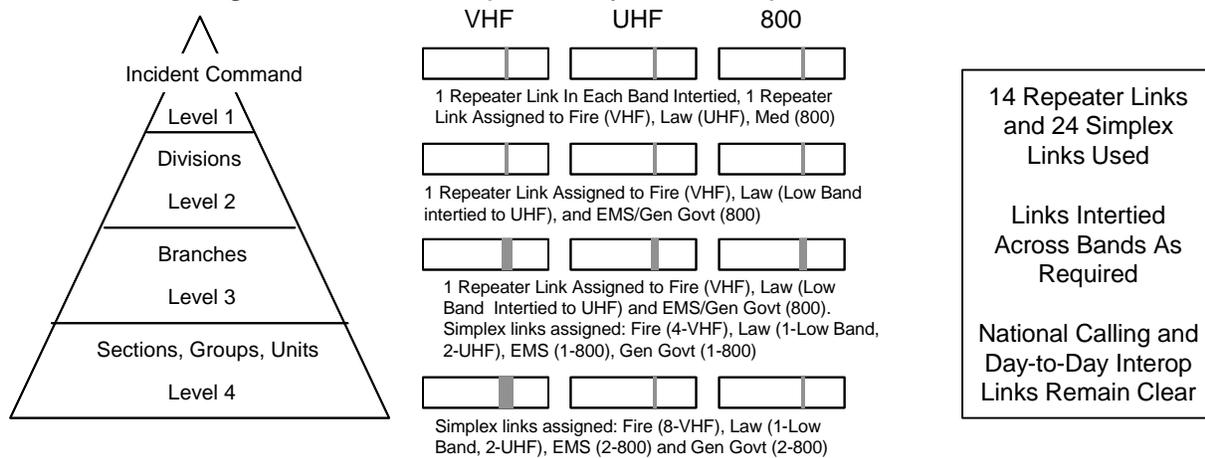
The FCC's National Coordination Committee for the 700 MHz band recognized this requirement, and the FCC embraced their recommendations when it recently incorporated the concept of State Interoperability Executive Committees (SIECs) into its regulations for the new 700 MHz band. That is not to say that States must control interoperability, rather that operational and technical requirements are best defined at the state level. SIECs will be most effective with broad representation from local, regional and state agencies within their boundaries. Proposals to expand the role of the SIECs beyond the 700 MHz band to include all spectrum assigned to local and State public safety agencies, as well as a number of Federal mutual aid channels, are now receiving wide support.

The following diagram provides the reader with an example of the interoperability links required to manage a major incident, in this case a large wildland fire similar to those that impact the western United States each year. This example was developed by the PSWAC after analyzing an actual incident in Southern California in the mid-1990s.

Figure 11-1. Interoperability for A Major Wildland Fire

VHF   UHF   800

Incident Command

Level 1

1 Repeater Link In Each Band Intertied, 1 Repeater Link Assigned to Fire (VHF), Law (UHF), Med (800)

Divisions

Level 2

1 Repeater Link Assigned to Fire (VHF), Law (Low Band intertied to UHF), and EMS/Gen Govt (800)

Branches

Level 3

1 Repeater Link Assigned to Fire (VHF), Law (Low Band Intertied to UHF) and EMS/Gen Govt (800). Simplex links assigned: Fire (4-VHF), Law (1-Low Band, 2-UHF), EMS (1-800), Gen Govt (1-800)

Sections, Groups, Units

Level 4

Simplex links assigned: Fire (8-VHF), Law (1-Low Band, 2-UHF), EMS (2-800) and Gen Govt (2-800)

14 Repeater Links and 24 Simplex Links Used

Links Intertied Across Bands As Required

National Calling and Day-to-Day Interop Links Remain Clear

Command Level 1: Nat Tac #R1 on VHF, UHF & 800 intertied as a command link for all disciplines. VHF Nat Tac #R2 is used for Fire Command, UHF Nat Tac #R2 is used for Law Command, 800 Nat Tac #R2 is used for EMS/Gen Govt Command.

Divisions Level #2: VHF Nat Tac #R3 is used for Fire, Low Band Nat Tac #R1 intertied to UHF Nat Tac #R3 used for Law, and 800 Nat Tac #R3 is used for EMS/Gen Govt.

Branches Level #3: VHF Nat Tac #R4 is used for Fire, Low Band Nat Tac #R2 is intertied to UHF Nat Tac #R4 for Law, and 800 Nat Tac #R4 is used for EMS/Gen Govt. VHF Nat Tac #S1 to S4 assigned to Fire, Low Band National Tac #S1and UHF Nat Tac #S1 and #S2 assigned to Law, 800 Nat Tac #S1 assigned to Medical, 800 Nat Tac #S2 assigned to Gen Govt.

Section/Group/Unit Level #4: The following are assigned for use by branches, groups and units: VHF Nat Tac #S5 to #S12 for Fire, Low Band Nat Tac #S2 plus UHF Nat Tac #S3 and #S4 to Law, 800 Nat Tac #S3 and #S4 for Medical and 800 Nat Tac #S5 and #S6 for Gen Govt.

This diagram depicts a typical assignment of Future Mutual Aid Spectrum Resources to a Major Wildland Fire Incident in Southern California

Interoperability Obstacles

In the technology arena, local, state and federal agencies are split across nine major frequency bands. At best, public safety radios fielded today can cover two or three of these bands. Even if your system shares the same band with your neighbors, systems are implemented in different incompatible technologies by different manufacturers; this is particularly true for trunked radio systems.

In the operational arena, we choose to use different protocols and naming conventions. While the fire service has generally standardized nationally on the Incident Command System (ICS), law enforcement still "does its own thing" in different areas of the country. They install compatible channels in their radios and then agencies name them different names; the field officer doesn't know the technical details and just assumes they won't talk to each other! Finally, agencies rarely train together using the interoperability channels and so, when a major event occurs, must start from scratch on how to make it work.

Perhaps the most difficult obstacles to overcome are in the political arena. Fire and police agencies often don't see a need to intercommunicate. There are turf differences between agencies, and not just at the agency head level, but between field officers as well… between police officers and sheriff's deputies, between park police and highway patrol, and the list goes on. However, when a major incident happens, everyone works together and works together well - they get the job done to the best of all their abilities - and the rivalries disappear. Just think how much better and more efficient they could do that job if they could intercommunicate and did it often enough that it was second nature.

But the politics list goes further. It goes to long-standing friendships between agency heads and/or purchasing managers and radio suppliers that lead to the purchase of an incompatible system, even though all of your neighbors share a common technology. And it goes to local control… it has to be "my system" even though a regional system may be more effective and efficient, both operationally and financially.

Interoperability Solutions

The key to successfully implementing interoperability is to carefully examine current systems and communications links, and identify where additional links need to be established and what the technical and operational parameters are that apply in each instance.

Classes of Systems

There are several major classes of systems. The characteristics, requirements and limitations of each are generally summarized as follows:

Conventional Systems:

1. Can make use of simplex and/or repeater-based operations.

2. All subscriber units must be in same RF band.

3. Secure communications usually requires equipment from same vendor.

Analog Trunked Systems:

1. Currently available only in 400 MHz band for Federal agencies and 800 MHz band for State/local agencies.

2. Proprietary systems require subscriber equipment from the same manufacturer (or a licensed second-source provider).

3. Secure communications usually requires equipment from the same vendor.

Project 25 Digital (Conventional or Trunked):

1. Vendor independent (including secure mode).

2. Infrastructure not required for conventional operation.

3. Some advanced features may be proprietary to a particular manufacturer.

Infrastructure-Based Patching:

1. Necessary only in following cases:
    a. Non-compatible (generally trunked or secure) systems
    b. Subscriber units on different RF bands

2. Requires one RF channel on each participating system, but can waste spectrum, especially for day-to-day operations.

3. Not usable when out of range of infrastructure (remote areas, etc).

4. "Interoperability" radio coverage is only available in the coverage area that is common to all participating systems.

5. Provides control that may not be present with other technologies.

Cost

Even if the previously described barriers can be overcome, the issue of funding often overshadows the others. Changes are often expensive and must be planned far in advance. Government funding cycles are long and the processes arduous. It is not uncommon that, by the time a budget is approved, the proposed equipment is old technology. Fortunately, the events of September 11 have highlighted the need for federal assistance to local and State first responders. There will be financial relief, at least for the next few years, and public safety agencies must take advantage of this opportunity.

As a national priority, the ultimate goal for interoperability must be that the field officer has it "on the belt" and knows how to use it when an event occurs. There should be no delay in their ability to talk with whom they need to talk to when they need to talk to them.

That said, getting there is a difficult and expensive road to follow. Estimates place the interoperability price tag at about $18 billion for local and State agencies. And, the road is different for each of the over 45,000 first responder agencies in the United States. Interoperability is hampered by the diversity of public safety spectrum and differences in the technology each agency has chosen to implement.

General consensus is that, until an affordable all-band, multi-mode subscriber radio is available, the best solutions to interoperability will be (1) regional harmonization of RF band and chosen technology - the preferred method, and (2) a system of cross-band patching of infrastructure. Though typically much less expensive (a 12-channel any-band patch system can be implemented for about $75,000), this latter choice is less desirable because of the large amount of spectrum required in a major event and because patching systems are only effective within the common coverage area of all participating users, as highlighted above.

Ultimately, the most successful technical solution to interoperability, even if affordable, will not be effective without appropriate operational procedures and regular training and/or use.