FEDERAL LAW ENFORCEMENT
WIRELESS USERS GROUP
WASHINGTON. D.C.

DOCKET FILE COPY ORIGINAL

April 26, 2000

RECEIVED

APR 26 2000

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Magalie Roman Salas
Secretary
Federal Communications Commission
TW-A325
445 Twelfth Street, SW
Washington, DC 20554

Re: Comments in Response the Commission's Notice of Proposed Rulemaking, *In the Matter of the 4.9 GHz Band Transferred from Federal Government Use*, in WT Docket No. 00-32

Dear Ms. Salas:

On behalf of the Federal Law Enforcement Wireless Users Group (FLEWUG) and pursuant to Section 1.419 of the Commission's rules, 47 C.F.R. § 1.419, enclosed herewith for filing are an original and four (4) copies of the FLEWUG's Comments in the above-referenced proceeding.

Kindly date-stamp the additional, marked copy of this cover letter and return it in the envelope provided.

Should you require any additional information, please contact the undersigned.

Respectfully submitted,

James J. Flyzik
Deputy Assistant Secretary
(Information Systems), and
Chief Information Officer,
Department of the Treasury, and
Vice Chair, Government Information Technology
Services Board

No. of Copies rec'd 0+4
List ABCDE

Before the
Federal Communications Commission
Washington, DC 20554

RECEIVED

APR 26 2000

OFFICE OF THE SECRETARY

In the Matter of	)	
The 4.9 GHz Band Transferred from Federal Government Use	)	WT Docket No. 00-32

FEDERAL LAW ENFORCEMENT WIRELESS USERS GROUP'S COMMENTS IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

1. The Federal Law Enforcement Wireless Users Group (FLEWUG)[1] respectfully submits comments on the Commission's Notice of Proposed Rulemaking, *In the Matter of the 4.9 GHz Band Transferred from Federal Government Use* (4.9 GHz NPRM).[2] In the 4.9 GHz NPRM, the Commission proposes to allocate and establish licensing and service rules for the 4940-4990 MHz band (4.9 GHz band) that has been transferred from the Federal Government for private use.

[1] The FLEWUG is comprised of law enforcement and public safety officials from the Department of the Treasury, Department of Justice, Department of the Interior, Department of Agriculture, Department of Defense, Department of Health and Human Services, United States Postal Service, United States Postal Inspection Service, National Telecommunications and Information Administration, Federal Emergency Management Agency, Internal Revenue Service, Federal Bureau of Investigation, United States Secret Service, United States Coast Guard, United States Capitol Police, Drug Enforcement Administration, United States Park Police, Immigration and Naturalization Service, United States Customs Service, Bureau of Alcohol, Tobacco, and Firearms, United States Mint, National Communications System, Defense Information Systems Agency, National Security Agency, Federal Law Enforcement Training Center, Bureau of Engraving and Printing, United States Marshals Service, National Institute of Standards and Technology, United States Forest Service, United States Fish and Wildlife Service, Federal Bureau of Prisons, Bureau of Land Management and National Park Service.

[2] The 4.9 GHz Band Transferred from Federal Government Use, WT Docket No. 00-32, *Notice of Proposed Rulemaking*, FCC 00-63 (rel. Feb. 29, 2000) (4.9 GHz NPRM).

I. STATEMENT OF INTEREST

2. In 1993, the Office of the Vice President issued a National Performance Review (NPR) report recognizing the need to improve public safety wireless communications. The NPR and a subsequent Memorandum of Understanding between the Department of Justice and the Department of the Treasury formally established the FLEWUG. The FLEWUG membership consists of more than 30 federal departments and agencies with law enforcement and other public safety responsibilities. Key among the FLEWUG's objectives is to plan and coordinate future, shared-use, wireless communications systems and resources. To this end, the FLEWUG supports development of shared-resource, shared-use, wireless communications systems; efficient use of the spectrum; and interoperability among local, state, and federal public safety agencies.

3. Given its mission, the FLEWUG has a clear interest in the proceedings related to the 4.9 GHz NPRM, particularly with respect to the viability of this band to help meet public safety's critical un-met spectrum requirements. Therefore, the FLEWUG offers the following comments to address several issues raised by the Commission.

4. Specifically, the FLEWUG takes issue with the Commission's assertion that setting aside spectrum in the 4.9 GHz band for public safety use is unnecessary due to the recent allocation of 24 MHz of spectrum in the 764–776 MHz and 794–806 MHz bands (the 700 MHz band) and the Commission's proposal to auction the entire band, noting that this band is viable to help alleviate the vital needs of the public safety community. Secondly, the FLEWUG suggests that if the currently scheduled auction of the 4.9 GHz band does not prove commercially viable, the Commission consider allocating a portion of the 4.9 GHz band for public safety use.

II. SIGNIFICANT PUBLIC SAFETY SPECTRUM SHORTFALLS REMAIN, AND THE 4.9 GHz BAND IS A VIABLE OPTION TO ADDRESS THESE SHORTFALLS

5. The FLEWUG reminds the Commission that the Public Safety Wireless Advisory Committee (PSWAC), whose participants included members of the state and local public safety community as well as the FLEWUG, were tasked by the FCC with determining the requirements

for public safety spectrum through 2010.[3] After extensive deliberations and research, the PSWAC determined that the public safety community would need an additional 97.5 MHz of spectrum to meet the demands placed on public safety communications[4]. Comparing the 24 MHz of spectrum in the 700 MHz band allocated to public safety under the Balanced Budget Act of 1997 (BBA 97) against the PSWAC recommendations, an additional 73.5 MHz of spectrum is still needed to meet public safety requirements through 2010, including 67.2 MHz of spectrum dedicated to wideband, high speed data and video applications by the year 2010.[5]

6. In the PSWAC Report, a number of frequency bands were identified as possible candidates for use by public safety agencies to satisfy their wideband, high speed data and video needs.[6] One such band was the 4.6 GHz band identified for reallocation pursuant to the Omnibus Budget Reconciliation Act of 1993 (OBRA 93). Subsequent to the release of the PSWAC report, the 4.9 GHz band was substituted for the 4.6 GHz band as a target for OBRA reallocation, and the FLEWUG contends that it would thereby be as viable a candidate for public safety use as the 4.6 GHz band. As a first step in satisfying the remaining wideband spectrum requirements, the FLEWUG suggests that the Commission consider reallocating spectrum in the 4.9 GHz band for public safety wideband, high speed data and video applications. If the Commission, in its deliberations, chooses not to provide a portion of the 4.9 GHz band to public safety, the FLEWUG urges the Commission to consider public safety's unmet spectrum needs in other portions of the radio frequency (RF) spectrum suitable for wideband, high speed data and video applications.

7. The FLEWUG believes that wideband, high speed data and video technologies can support a number of public safety applications such as imaging and real-time video which are becoming increasingly more important to public safety as technology develops and demands shift. Agencies use these technologies to support activities such as geographic positioning,

---

[3] *Final Report of the Public Safety Wireless Advisory Committee to the Federal Communications Commission*, Reed E. Hundt, Chairman, and the National Telecommunications and Information Administration, Larry Irving, Assistant Secretary of Commerce for Communications and Information (PSWAC *Final Report*) (1996).

[4] The FLEWUG observes that all or part of the 24 MHz allocated under BBA 97 may never be available for public safety usage in some regions due to new or incumbent users occupying the spectrum indefinitely.

[5] Public Safety Wireless Network (PSWN) Program, *Public Safety Radio Frequency Spectrum: Highlighting Current and Future Needs* (January 2000), See footnote 5 at 1.

[6] PSWAC Final Report at 641.

automatic vehicle location, report transmission, electronic messaging and accessing data repositories such as the National Crime Information Center. Typical images transmitted by public safety users include building plans, mug shots, fingerprints, and snapshots of accidents, injured persons, and crime scenes. Agencies use video primarily to monitor critical public safety incidents such as criminal surveillance, major fires, and prison riots. Video is also used for day-to-day activities such as highway monitoring. The use of new technologies not only enhances the capability of individual units and agencies, it also has facilitated local, state, and federal agencies' capacity to interoperate in complex multijurisdictional situations such as high-speed pursuits or drug interdiction.[7] In short, these applications will assist public safety providers at all levels of government to save lives and protect property.

8. Even though these applications can enhance public safety's capabilities, the FLEWUG asserts that the public safety community currently only makes limited use of wideband, high speed data and video due, in large part, to the lack of spectrum needed to implement these systems. This trend of limited use is expected to change as evidenced in a recent survey where fire and emergency medical services (EMS) personnel revealed that their use of wireless data applications would increase over the next two years by as much as 400 percent.[8] However, with only one video channel presently available for public safety use, this projected growth will be hampered.[9] Unless addressed immediately, the lack of broadband spectrum will significantly affect public interest by impeding the implementation of wideband, high speed data and video technology for public safety operations.

9. The FLEWUG would like to offer the Commission further evidence of public safety's need for wideband, high speed data applications by highlighting the activities of several independent groups who are attempting to address this issue. First, Project 34, a user-driven standards setting effort, is in the process of developing a statement of requirements (SOR) for wideband mobile digital radio technology standards for public safety equipment. This group, consisting of both manufacturers and members of the public safety community, is developing recommended standards that allow for half- and/or full-duplex transmission of digital

[7] PSWN Program, *Public Safety Radio Frequency Spectrum: Highlighting Current and Future Needs* (Jan. 2000) at
[8] PSWN Program, *Analysis of Fire and EMS Communications Interoperability*, April 1999, at 32.
[9] PSWAC, *Final Report* at 213.

information at gross channel data rates between 1.544 Mbps and 155 Mbps.[10] This will allow for such applications as real-time high resolution video and wireless internet access. The goal of this group is to bring both users and manufacturers together to meet the unique operational demands of public safety. A current version of the SOR is attached.

10. In addition, the Public Safety National Coordination Committee (NCC) has established a working group to specifically identify public safety's wideband, high speed data requirements and recommend a standard to facilitate the development and deployment of these applications. In a briefing presented at the NCC meeting in January, it was shown that the bandwidth consumption for public safety data and voice applications is expected to continue increasing.[11] Point-to-point communication systems that can be used to link remote radio sites will have data rates in the 1.544 Mbps (equivalent to T-1 landline data rates) or higher. It is estimated that good quality video requires a data rate of at least 1 Mbps for two-way operation. Therefore, even if higher-order modulation schemes[12] and data compression techniques[13] are employed, channel bandwidths greater than 150 kHz will still be necessary, making the current 700 MHz allocation of 24 MHz unsuitable for advancing technology as channel widths permitted in this band are limited to 150 kHz.

11. The Commission has sought comment on its tentative conclusion not to allocate any portion of the 4.9 GHz band for public safety use. The Commission has ostensibly based this conclusion on the assumption that the recently allocated 24 MHz spectrum in the 700 MHz band will adequately serve future needs of the public safety community.[14] As discussed above, the FLEWUG disagrees with this assumption and believes that current spectrum allocation falls short of meeting the public safety community's requirements because the broadband data channels in the 700 MHz band have been assigned a maximum channel bandwidth of

---

[10] Project 25/34 New Technology Standards Project SOR, *Wideband Aeronautical and Terrestrial Mobile Digital Radio Standards for the Wireless Transport of Rate Intensive Information* (June 1, 1999) at 3.

[11] Briefing to the NCC Technology Subcommittee: *746-806 MHz Wide Band Data*, Tim Goodall Motorola Wireless Solutions Market Planning Manager (Jan. 13, 2000) at 9.

[12] Higher-order modulation schemes allow transmission of more information over a constant bandwidth.

[13] Data compression techniques reduce the number of bits that must be transmitted.

[14] See *4.9 GHz NPRM* at ¶ 26.

150 kHz.[15] The wideband, high speed data and video systems that public safety agencies intend to use to support their missions will require bandwidths that are wider than 150 kHz (the FLEWUG does not support channel widths higher than 150 kHz on the 700 MHz band). Therefore, the FLEWUG recommends that the Commission establish a new allocation with adequate bandwidth that will allow manufacturers to begin developing the equipment necessary to meet the needs of the public safety community.

III. PUBLIC SAFETY AGENCIES SHOULD BE AWARDED SPECTRUM IN THE 4.9 GHz BAND IF AUCTIONS PROVE NOT TO BE COMMERCIALLY VIABLE

12. The Commission has tentatively concluded that spectrum in the 4.9 GHz band will be acquired through competitive bidding.[16] The FLEWUG does not challenge this determination. However, the FLEWUG also asserts that the competitive bidding requirement should not apply to public safety agencies because it is the FLEWUG's understanding that this would be contrary to Congressional direction, as codified in BBA 97, which exempted the public safety radio service from participating in spectrum auctions.[17] Congress' decision to exempt public safety agencies from spectrum auctions was based on the fact that spectrum auctions deprive state and local government public safety agencies of any opportunity to obtain new radio spectrum for their critical police, fire, emergency medical, and other communications systems. In making this decision, Congress correctly recognized that several obstacles impede public safety agencies' participation in the competitive bidding process. These obstacles include the limited monetary resources and administrative capabilities of public safety agencies.

13. In light of these factors, the FLEWUG suggests a different approach for the Commission to couple public safety spectrum needs with spectrum auctions. The FLEWUG recommends that the Commission allocate, at no cost, spectrum within this band to public safety agencies if the Commission does not garner the revenue that budget analysts expect in the auction process.

---

[15] The Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010 and Establishment of Rules and Requirements for Priority Access Service, WT Docket No. 96-86, *First Report and Order and Third Notice of Proposed Rulemaking*, 14 FCC Rcd 152 (1998) at ¶ 40.

[16] 4.9 GHz NPRM at ¶ 94.

[17] BBA 97, Pub. L. No. 105-33, 111 Stat. 251 § 309(j)(2).

FLEWUG asserts the public interest would be better served by allocating this spectrum, at no cost, for public safety use instead of accepting negligible auction revenues. In effect, FLEWUG is suggesting a default allocation be made to public safety in lieu of an auction that would not yield significant revenue.

IV. CONCLUSION

14. The FLEWUG strongly urges the Commission to reconsider its tentative conclusion that the 24 MHz of spectrum allocated under BBA 97 is sufficient to support public safety community's need for wideband, high speed data and video, and suggests that the 4.9 GHz band would be a viable candidate for this type of use.

15. The FLEWUG recommends that the Commission consider allocating a portion of the 4.9 GHz band to public safety usage if the auction process does not prove to be commercially viable.

Respectfully submitted,

James J. Flyzik
Deputy Assistant Secretary
(Information Systems), and
Chief Information Officer,
Department of the Treasury, and
Vice Chair, Government Information Technology
Services Board

Project 25/34 New Technology Standards Project

Statement of Requirements

Wideband Aeronautical and Terrestrial Mobile Digital Radio Technology Standards
For the Wireless Transport of Rate Intensive Information

June 1, 1999
Revision 4.00

Forward

This Statement of Requirements document includes a general outline of the public safety community's technology needs for the transport and distribution of rate intensive data, digital video and digital voice for both service-specific and general applications. This standards effort is intended to support implementation of the federal government's Public Safety Wireless Network (PSWN) initiative.

The convergence of voice and data services is revolutionizing the commercial transport of information, both wired and wireless. To date, this convergence has had minimal impact on the dedicated systems employed by most public safety agencies. This Statement of Requirements anticipates that convergence will be a natural progression within the public safety community as new, rate intensive technologies are implemented.

The initial gross data rates identified in this document are for 3rd generation wireless technologies. However, requirements identified herein are intended to clearly identify the migration path to 4th generation technologies and beyond.

The *Final Report* of the Public Safety Wireless Advisory Committee (PSWAC)[1] is a major source document for this Statement of Requirements. Within the *Final Report*, the four generally universal limitations of priority access and system restoration, reliability, ubiquitous coverage, and security were identified as restricting the use of commercial services for mission critical public safety wireless applications.[2] This Statement of Requirements is intended to describe a platform that can be installed as a government/commercial partnership that overcomes these limitations, providing universal access to all subscribers within a carefully controlled and managed network.

---

[1] The Public Safety Wireless Advisory Committee was jointly chartered on June 25, 1995, in accordance with requirements of the Federal Advisory Committee Act by the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA) to examine the operational and spectrum needs of federal, state and local public safety agencies through the year 2010 and to make recommendations for meeting those needs. Its *Final Report* was released on September 11, 1996.

[2] *ibid*, Section 1.23, p 14. Additionally, *Final Report* Appendix C (Interoperability Subcommittee Report) Sections 1.2.4, 3.3 and 6.1.3 and Appendix D (Spectrum Resources Subcommittee Report) Section 7.3 provide detailed technical discussions about these limitations.

For the purpose of this Statement of Requirements, public safety includes criminal justice, emergency management, emergency medical services (EMS), fire, land and natural resource management, military, transportation, wildlife management, and other similar governmental functions that have a need for aeronautical and terrestrial mobile wireless communications.

I. Introduction

The objective of this Project 25/34 Statement of Requirements (SOR) is to establish, from the user's perspective, a standards profile for the operation and functionality of new aeronautical and terrestrial wireless digital wideband public safety radio standards that can be used for the transmission and reception of voice, video, and high speed data in a ubiquitous, wide-area, multiple agency network. Some of the primary attributes of this network(s) would include, but not be limited to, the following:

A. Satisfies the current and identified long-term needs and requirements of the local, state and federal public safety communities.

B. Affords immediate, significant and evolutionary improvements in radio bandwidth and spectrum efficiency.

C. Promotes competition in system life-cycle procurements.

D. Permits effective, efficient, reliable and, as required, secure (authenticated and/or encrypted) intra- and interagency communications (interoperability).

E. Provides ergonomically designed, human engineered "user friendly" equip-ment.

F. Establishes a digital tactical communications architecture that provides for a "migration-in-place" transition within existing systems, effected through full backward interoperability/compatibility with existing analog and digital wireless communications systems used by local, state and federal agencies.

G. Is consistent with Project 25 Phase I and Phase II and parallel federal standards.

H. Provides an architecture capable of transporting multiple international standards-based data protocols.

I. Allows for the half and/or full duplex transmission of digital information at gross channel data rates of up to a minimum of 1.544 megabits per second (Mbits/s, 3rd generation), and 155 Mbits/s or higher for 4th generation technologies.

J. Allows for the seamless hand off of subscriber units moving between fixed sites.

K. Allow for multiple levels of security, network integrity, and availability.

L. Provide for a network design that is capable of rapidly passing traffic with minimum errors through various harsh environments.

M. System and network switching that will allow subscriber units to access the particular network(s) they are authorized to access.

II. General Requirements

The following represents an overview of Project 25/34 wireless aeronautical and terrestrial mobile wideband high-speed data, video and voice standards general requirements:

A. The wireless standards must accommodate the creation of a new multiple-agency, multiple-function, multiple-services mobile computer telecommuni-cations system and associated network(s).

B. The wireless standards will be used for proposed public safety networks and subscriber units that are designed to transfer digital voice, data and video at high data rates, between and among wireless mobile data terminal units and with fixed terminal units. The fixed terminal units will be interconnected to a variety of networks, and mainframe and host processors.

C. The wireless standards should be fully digital, based upon existing protocols employing both information rate arbitration and adaptation techniques to permit seamless transport of digital information between and amongst systems.

D. The wireless standards developed from this SOR must be driven by the objective of providing a complete suite of wide area "in vehicle" and portable "in building" services employing an assortment of technologies, including: wide area synchronous simulcast, wide area multicast, distributed satellite receiver voting, macrocell and microcell technologies.

E. The wireless standards must ensure nationwide interoperability between high information transfer rate network elements.

F. The wireless standards must ensure nationwide interoperability between individual subscriber units located beyond the range of operational infrastructure.

G. This SOR shall use standardized technology that will allow subscriber units to interface directly with "off-the-shelf" notebook and hand-held computers and with personal digital assistants (PDAs) and similar evolving mobile and personal data products.

H. Adopt an Open System Architecture and Design approach and employ "best practices" for implementation where standards are not yet established.

I. The wireless standards developed in accordance with this SOR should embody a long-term wireless subscriber unit and network strategy that includes a transparent migration path to the widespread use of mobile, notebook and hand-held computers and PDAs, with both on-net and off-net priority communications, and point-to-point and point-to-multipoint video.

J. The ultimate standards must embody the concept of connecting to, or interconnecting with, all major national and state high information transfer rate public safety data platforms and applications as may be defined elsewhere in this SOR.

K. The wireless standards must provide dynamic network optimization.

L. The wireless standards shall be frequency neutral, thereby allowing standard-ized technology to be used in any authorized and available public safety spectrum, consistent with available radio frequency channel bandwidth.

M. The wireless standards shall be developed to ensure an adequate level of interference protection to and from adjacent systems and/or channels. Adequate interference protection is defined as that which is sufficient to permit operation of a system within the specified interference-limited system design parameters.

N. The wireless standards will be written to comply with both Federal Communications Commission (FCC) Rules and Regulations and with applicable regulations of the National Telecommunications and Information Administration (NTIA) unless otherwise agreed to by the majority of the concerned parties in the standards development process.

O. While wireless standards referred to in this SOR are written for the specific use of local, state and federal public safety agencies, there is nothing within these requirements, or intended by these requirements, that precludes any or all of the standards from being used in other general land mobile radio applications.

P. The wireless standards developed from this SOR should include in their development process consideration of the requirements of the following federal guidelines and recommendations:

- The Federal Bureau of Investigation (FBI) National Crime Information Center (NCIC) 2000 System Requirements.
- The FBI's Integrated Automated Fingerprint Identification System (IAFIS) System Requirements Definitions.
- The FBI's IAFIS concepts of operations.
- The FBI's Integrated Digital Wireless Communications System (IDWCS) Performance Specification
- The FBI's Technology Planning Guide.
- The National Incident-Based Reporting System Requirements for use of the handbooks for Uniform Crime Reporting, Volumes 1 through 4.
- The Federal Data Collection Guidelines - Volume 1.
- The Federal Data Submission Specifications - Volume 2.
- The Federal Manual on Approaches to Implementing an Incident-Based Reporting

System - Volume 3.

- Federal Guidelines on Error Message Manual - Volume 4.
- Federal Guideline Hate Crime Data Collection.
- OMB Circular A130 as it applies to interoperability requirements between federal and state governments for Automated Information System security.
- The Immigration and Naturalization Service's ENFORCE concept of operations.
- The *Final Report* of the Public Safety Wireless Advisory Committee.

This material provides examples of the federal system and federal system's requirements that will need to be considered in developing an "open" network interface. Although all of these documents do not directly relate to the proposed wireless standards, they all relate the type of data files and applications that will be remotely accessed by the standardized high-speed wireless hardware proposed within this SOR. The inclusion of this material in this SOR is not and should not imply, nor is it intended to suggest, that the proposed standards must comply with all the material contained therein. In fact, some of this material may have already been superseded and/or is in direct conflict with the purpose of this SOR. However, for the purpose of this document, these references show a limited snapshot of the networks and application with which a standardized wireless network will need to interface, as well as associated interoperability problems.

Q. The technology selected to meet this SOR must be capable of supporting information transfer rate intensive applications such as the rapid transmission (e.g., within three seconds) of digital photos taken at the scene of a public safety incident.

R. The wireless standards should include technology that will accommodate the simultaneous transmission and reception of high information transfer rate split screen data to/from a mobile terminal unit.

S. The wireless standards will take full advantage of the Global Positioning System (GPS) for the synchronization of networks and the management and deployment of resources.

T. The wireless standards must embody technology that can interface with other wired and wireless public and private networks, including the public switched telephone network (PSTN) using accepted industry standards.

III. Operational Requirements

This partial list of system and user applications has been included in the Project 25/34 SOR to establish a base line for standardized technology. Many of the items referenced are taken directly from the *Operational Requirements Subcommittee Report* (Volume II, Appendix A) of the Public Safety Wireless Advisory Committee (PSWAC) *Final Report*. In addition, specific requirements of local, state and federal agencies have been added. This list is not intended to be restrictive or to preclude other applications or needs. Further refinements will take place within the Project 25/34 process as the standards are being developed. Therefore, Project 25/34 standards should be designed to accommodate, but not be limited to, the following types of applications.

A. Common Features Desired by All Disciplines

All public safety disciplines have indicated a need, to some extent, for the following data and video services. Wireless communications support is crucial to assure quality services and create the safest possible working environment for public safety personnel and for the public they serve.

1. Data

The basic requirement for data is the immediate, error-free transfer and display of text and graphical information for all personnel, in support of both routine and emergency operations, prioritized according to need.

a. Mobile/Personal Data Computer/Terminal Applications. A need exists for real-time support of wireless mobile and portable computer systems capable of transmitting and receiving routine data queries and responses, electronic mail, location data and other graphics, along with incident-specific data and intelligence, and command and control information.

b. Electronic Messaging. Personnel require the ability to input messages into a data transmission device for transmission to single or multiple agencies, including other personnel and other public safety providers.

c. Geographic Position and Automatic Location Data. Per-sonnel require the ability to transmit location data, determined by geographic position technology or other means, automatically or on demand, to other locations. Examples of this need include constant updating of vehicle positions for dispatch and personnel safety purposes, constant updating of individual officer location for safety purposes when the officer is outside of her/his vehicle, and the ability to trigger position transmitting devices on lost or stolen equipment items. Many of these applications require secure transmission of the position information to protect operations from compromise by potential adversaries.

d. Transmission of Reports. This system should accommo-date transmission of forms and reports to central sites from mobile and remote locations. This capability will be used to transmit various types of forms and reports to central locations in long data streams of up to several seconds. This capability will reduce paper transactions, increase field time, and speed transmission of vital information to command and administrative staff.

e. Additional details on data requirements are included in Appendix A.

2. Video

With major incidents, multiple agencies often need to be able to monitor another agency's video transmissions, but the ability to access public safety video must be based on a "need-to-know" or incident management basis.

a. Aerial Video. Airborne video platforms provide critical support and intelligence for major events, in particular for disaster response and management. Near-full motion and snapshot video transmissions from airborne platforms to command and control locations and supervisors on the ground are required.

b. Incident Video. Some incidents require real-time video. While these incidents may be infrequent in some areas and some disciplines, others have a more frequent demand for real-time video. The capability must exist for both point-to-point and broadcast use of the video. For example, full motion video must be transportable from the incident scene to an incident command post, and also to a remotely located emergency operations center. Major incidents often require monitoring of the incident from more than one location.

c. Still-Photographs. Agencies require the ability to transmit still photographs on demand to other locations. For example, a law enforcement, parole or probation officer in the field should be able to transmit and/or receive a digital image of probationers or parolees to and/or from other officers and central dispatch points.

d. Additional details on data requirements are included in Appendix B.

The following pages detail more specifically the data and video requirements for the seven (7) major public safety categories.

B. Criminal Justice Services (Corrections, Courts, Law Enforcement)

Reducing crime and its impact on the health and welfare of families continues to be a top priority in the United States. In recent years, the most successful anti-crime weapon in the criminal justice arsenal has been implementation of community-based policing in many areas of the country. The heart of this program is getting officers out of cars and into the community, whether it be on foot, bicycle or horseback. Community-based policing programs put an extraordinary demand on communications systems because they require portable coverage throughout the community. Additionally, the 100,000 new officers funded through the Violent Crime Control and Law Enforcement Act of 1994 (Public Law 03-322, commonly called the "Crime Bill") must be community policing officers. The additional load placed on already overworked communications systems by these new officers has been noticeable.

Expansion of wireless data systems offers many technological assets for law enforcement information, stolen articles, and criminal histories. Repository systems such as the National Crime Information Center (NCIC) 2000 system and the Integrated Automated Fingerprint Identification System (IAFIS) are preparing to provide mission critical data to law enforcement more effectively and efficiently; they will certainly prove to be a force multiplier in the war on crime. For the first time, authorized field officers will be able to positively and rapidly confirm the identity of persons in the field by transmitting a fingerprint to state or federal processing centers. The officer will be able to obtain a photograph of any person who has been cataloged by these systems.

Future information technology requirements for state and local law enforcement will most certainly include wireless data and voice systems utilizing encryption. In order to maximize the effectiveness of personnel in the field, a mobile office environment utilizing secure wireless data communications must be developed. This mobile office would provide instantaneous voice, data, and video access to other criminal justice personnel, various law enforcement data repositories, personnel from other public safety disciplines, and commercial networks. At some point, law enforcement may incorporate these mobile offices into a paperless environment inclusive of multimedia transfer.

Correctional organizations across the country are a mix of both sworn and non-sworn personnel and have a unique and varied public safety mission. The operational public safety radio communications needs of correctional organizations will mirror one or more of those of all of the other commonly recognized public safety and public service organizations. Correctional organizations provide public safety in the forms of law enforcement, fire services, emergency medical services, emergency management and disaster services. They also provide public service in the forms of highway maintenance, fire prevention, conservation, the reintegration of offenders back into society, and community public works.

Prisons and jails can be viewed as small but fully autonomous communities. In addition to the custody staff, a variety of support staff are needed. Cooks, laundry workers, firefighters, doctors, dentists, educators and maintenance personnel are needed to ensure inmates are housed, clothed, and fed accordingly. Activities, tasks, and communications that may appear mundane, routine or administrative in normal circumstances take on significant public safety and security implications in the correctional environment.

Beyond the common requirements detailed in (A) above, Criminal Justice Services have the following unique requirements:

1. Law Enforcement Data

Based upon the rapid market penetration of portable two-way radios into law enforcement ranks in the 1970's, the International Association of Chiefs of Police (IACP) Communications Committee has presented the possibility that over 75% of the nation's state/local police forces could be equipped with portable data terminals in the 2005-2010 time frame, given that affordable equipment and the required infrastructure and spectrum become available.

2. **Law Enforcement Video**

a. Robotics Video. Hazardous material and explosive disposal response frequently benefits from use of robotic devices. Full motion, generally short distance (up to 1000 meters), video transmissions from the robotic device to a locally-located control site is required to support such robotics activities. This application may require the use of equipment and technologies developed for explosive atmospheric conditions and/or that will not initiate the explosive device being rendered safe.

b. Surveillance and Monitoring. Law enforcement requires the ability to transmit high resolution, limited motion video at the rate of one frame every five (5) seconds for surveillance and monitoring purposes. For example, person and building surveillance, low risk drug transactions, and building security would be adequately served by this quality of video transmission.

c. Officer Safety and Operational Video Transmission (Two Way). The ability to transmit full motion video from mobile video cameras directly to dispatch and other command and control installations is required. Although the constant transmission of this data from each individual officer or mobile unit is not required, the ability to monitor video from a unit is needed on an episodic basis in the event of officer assistance situations and other high risk events, or operations of high command interest. In addition, the system must support retransmission of full motion video to mobile and remote locations, where command and control personnel and other mobile officers can monitor, perform decision-making and provide assistance based on the video transmission.

3. Jail & Prison Data

a. Mobile Data Computer/Terminal Applications. Portable, wireless access to facility floor plan layouts for fire suppression or the development of tactical assault plan for special teams is essential to save lives. When traveling away from correctional facilities, wide area mobile data applications are required to manage transportation routing and scheduling.

b. Geographic Position and Automatic Location Data. As correctional organizations must monitor larger and larger inmate populations with less and less staff, prisons and jails have identified a need to monitor individual inmate movement and location within large facilities. Such systems may also provide for early detection of escapes between physical counts. Outside of facilities, there is the need for constant updating of vehicle positions for transportation dispatch and transportation officer safety purposes.

c. Emergency Signals. Correctional personnel in prisons and jails who need emergency assistance must be able to activate an alarm that sends an automatic distress notice to a central monitoring point and other staff in the facility. The sophistication of such systems varies from simple "panic buttons" that will activate a general alarm, to more complex systems that incorporate multiple features such as unique unit identification, automatic unit registration, mercury activated person-down switches and automatic unit location. Often times these systems are stand-alone from other communications systems such as voice radio in order to provide staff security to those who would otherwise not require a portable communication device.

4. Parole and Probation Data

a. Geographic Position, Automatic Location Data, Remote Device Monitoring. A major role in incarceration is now being played out in the community by probation and parole organizations, where their charges are sequestered in their homes by remote electronic monitoring. This use of "house arrest" has risen tremendously. Additionally, there is a mounting movement to develop systems and process to continually monitor and know the whereabouts of probationers, parolees and early release inmates on a continuous basis. Proposed requirements have included a location accuracy of a few meters and a minimum five minute interval report time.

b. Emergency Signals. Probation and parole personnel who need emergency assistance must be able to activate an alarm that sends an automatic distress notice to a central monitoring point and other staff in the field.

5. Parole and Probation Video

a. Surveillance and Monitoring. As correctional organiza-tions must monitor larger and larger inmate populations with less and less staff, prisons and jails have identified the need to use real-time video to monitor multiple secure areas from remote locations. Additionally, remotely operated video cameras are a great asset in reducing the introduction of contraband into facilities via visiting room settings. There are some prison locations where wired video systems are not practical or where portable video systems requiring wireless links are required.

C. Emergency Management and Disaster Services

Communications system requirements for emergency management and disaster services are characterized by very low usage patterns during routine operations and extremely high usage patterns during a major event. Thus, radio systems designed and used by emergency management agencies appear to be virtually unused on a day-to-day basis, yet when a major event occurs, these same systems are inadequate for meeting the need to communicate. Although individual communications systems performed properly, incident needs still were not met

due to interoperability issues following the bombings in New York at the World Trade Center and in Oklahoma City, in Miami following Hurricane Andrew, in Los Angeles during the Rodney King riot, following the Loma Prieta and Northridge earthquakes, and countless other times.

We should not look at large-scale events as being an anomaly. True, major earthquakes do not occur that often. Nor do hurricanes or floods. Taken all together though, they occur more often than we would like to think. Furthermore, few years pass without a major forest or wildland fire such as those in Yellowstone National Park and in Malibu, California being battled by one thousand or more firefighters from hundreds of fire agencies. Special events such as the Olympics, political conventions, and the "Million Man March" occur each year. The reality is, large-scale events happen every year at unpredictable locations and at unpredictable times. Public safety agencies must be prepared to respond to these events when they occur and they need effective communications to aid in their response. While the unpredictability of these events makes it impractical to have adequate wireless communications facilities in place, we can identify and protect blocks of frequencies where such facilities can be rapidly implemented.

Beyond the common requirements detailed in (A) above, Emergency Management and Disaster Services have the following unique requirements:

1. Emergency Management Data

    a. Data applications for emergency management agencies will exist to a smaller degree prior to disasters, and become critical once a disaster occurs.

    b. Geographic Position and Automatic Location Data. Access to the Global Positioning System (GPS) is a valuable tool in a disaster.

Following an earthquake, flood, hurricane, or other disaster it is not uncommon for normal landmarks to have disappeared. Buildings are destroyed, streets are covered, and road signs are missing. Emergency management personnel need a means by which they can map the event so that they can better understand where the problems lie and dispatch personnel to deal with situations appropriately. Although access to the GPS signal itself does not create a path or channel requirement, use of location data at any other location requires that a communications link be established.

c. Interoperability Data. Disasters require the aid of a multitude of public safety and public service agencies to effectively save lives and protect property. Disaster intelligence is greatly enhanced by the ability to send and display information formatted as text and graphics. It is impossible to effect efficient command and control without the ability to communicate with assisting and cooperating agencies on major disasters.

2. Emergency Management Video

a. The availability of a variety of video/imagery sources is critical to the effective management of a disaster. For example, automatic aid agreements with commercial broadcast agencies would often provide quality video/imagery of incident scenes for command personnel, either directly or through retransmission.

b. Interoperability Video/Imagery. Video interoperability is a critical operational requirement. Disasters require the aid of a multitude of public safety and public service agencies to effectively save lives and protect property. Additionally, video and imagery is gathered from multiple sources, both public and private, during disasters. The ability to utilize video and imagery from multiple sources, as well as the ability to share this information among assisting and cooperating agencies, will greatly enhance emergency management operations.

D. Emergency Medical, Fire and Related Life and Property Protection Services

The mission of the Fire, Emergency Medical and Related Life and Property Protection Services includes those public entities that provide services to the public encompassing emergency life saving and the critical care of the sick and injured, as well as emergency property protection. Historically, these services have been categorized as Fire Service and Emergency Medical Service (EMS), and in many jurisdictions all or part of the functions contained herein are managed exclusively by Fire and EMS providers. Today, a number of agencies provide a broad scope of services including fire suppression and prevention, emergency medical paramedic, hazardous materials, urban search and rescue, technical and mountain search and rescue, swift water rescue, and ocean lifeguard services. This broadening scope of service displays significant growth from the historic perspective of fire suppression and first aid. Furthermore, this broadening requires transmission of secure information in such applications as property access and patient medical data.