

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" equipment.
- 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 telecommunications 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 inter-connecting 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 standardized 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. Personnel 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 accommodate 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 organizations 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.

Wireless command, control and communications support is crucial to assure quality life and property protection and to create the safest possible working environment for Fire, Emergency Medical and related Life and Property Protection services personnel. Wireless technologies are the emerging backbone of command, control, communications, and computerized synthesis of intelligence gathering and distribution (C4I.)

To represent all of these providers without regard to umbrella agency categorization, a description of unique operational requirements not detailed in (A) above is provided for each of the following life and property protection services:

Emergency Medical Services
Fire Suppression and Prevention
Hazardous Materials
Ocean Lifeguards/Blue Water Rescue
Swift Water Rescue
Urban Search and Rescue/Technical Search and Rescue

1. Emergency Medical Services (EMS)
 - a. Patient Care Data. A need exists for the wireless transfer of patient vitals and diagnostic data. Advanced diagnostic tools such as twelve lead EKG, EEG, ultra-sound, and MRI will transfer life saving information between field units and base hospitals.
 - b. Video/Image Requirements. Video/Image capture and display systems must be capable of transferring patient specific replications from units in the field to diagnostic patient care centers. The ability for doctors to view the actual patient in conjunction with voice and data assessment information will greatly enhance patient care and survivability.

2. Fire Suppression and Prevention
 - a. Aerial Observation Video/Imagery. A need exists for the transmission of video/imagery from airborne platforms to the incident command post. This need is especially critical for the management of large wildland fires.
3. Hazardous Materials (Haz Mat) Response
 - a. Robotics Support. In extremely hazardous situations, hazardous material containment may only be accomplished with remote equipment supported by robotics. The operation of this equipment will be heavily dependent upon wireless data connectivity.
 - b. Aerial Observation Video/Imagery. A need exists for the transmission of video/imagery and multi-spectral toxic cloud replication from airborne platforms to the incident command post.
 - c. Robotics Video/Imagery. In extremely hazardous situations, hazardous material containment may only be accomplished with remote equipment supported by robotics. The operation of this equipment will be heavily dependent upon wireless connectivity and the ability to guide these devices using wireless video links.
4. Ocean Lifeguards/Blue Water Rescue
 - a. Robotics Support. Lifeguards/Water Safety personnel often require the support of robotic devices in underwater search and rescue operations when persons, planes, and ships are submerged in water depths greater than 200 feet. Robotics equipment becomes the preferred method of retrieval as human divers require considerable decompression time at these depths. The utilization of remote control recovery vehicles eliminates the need to further risk human life to recover a dead body or salvage from ships or planes.
 - b. Robotics Video/Imagery. Where robotics support is used, the operation of this equipment will be heavily dependent upon wireless connectivity and the ability to guide these devices using video support. As with the law enforcement application, special equipment designs may be required.

5. Swift Water Rescue
 - a. Aerial Observation Video/Imagery. The transmission of incident information from airborne platforms to the incident command post and to rescue personnel is extremely valuable, particularly during major flood incidents.

6. Urban Search and Rescue/Technical Search and Rescue (USAR/TSAR)
 - a. Robotics Support. USAR/TSAR personnel often require the support of robotic devices in search and rescue operations when persons are trapped in collapsed buildings, mines, tunnels, etc. Robotics equipment may be the only method of locating trapped persons in areas where human rescuers are physically unable to enter because of access limitations or the presence of hazardous materials. The utilization of miniature remote control vehicles for such applications will dramatically increase in the future.
 - b. Robotics Video/Imagery. In extremely hazardous situations, rescues may only be accomplished with remote equipment supported by robotics. The operation of this equipment will be heavily dependent upon wireless connectivity and the ability to guide these devices using video support. As with the law enforcement application, special equipment designs may be required.

E. General Government

The needs of the General Government are diverse in nature since they perform a myriad of tasks to carry out their respective missions. The term "General Government" includes any United States territory, possession, state, county, city, town, village or similar governmental entity, including a district and an authority. The need is for essential communications necessary to fulfill official governmental responsibilities.

A major portion of this section is based on the needs of large urban regions since there are a broad range of uses in densely populated areas. In addition, the needs of surrounding suburban and rural areas were also taken into account for these regions. General Governmental services focus on legislative, community and general matters, all of which are a function of government.

Beyond the common requirements detailed in (A) above, General Government has the following unique requirements:

1. General Government Data Requirements

- a. Mobile and Portable Data Terminals. General Government requires field computers capable of remotely accessing information systems and files. Field computers may be used for dispatch or field support to perform real-time changes to system data. Equipment may be vehicle mounted or a hand held portable unit. Mobile unit status and control provide essential cost and time saving abilities to day to day operations. Administrative data transfer allows for information exchange for a work force that is remote and mobile.
- b. Data Transmission & Telemetry Systems. General Government requires real-time information transfer from field locations (fixed, mobile, or portable) to fixed control points. Transmission is used to monitor the functions of a system, site, or device. This may also incorporate a type of personal paging device used to alert personnel with limited alphanumeric messages. Some applications require use of transmission authentication and/or security.
- c. Remote Public Information Systems. Changeable signs and public information systems with the ability of the authorized entity are used to dynamically change visible street signs/bulletin boards and alert the public to potential hazards or delays.
- d. Vehicle, Personal, and Device Location Tracking. Location information allows more efficient use of equipment and personnel, equipment management inventory, and location control. The ability of dispatch control point or other vehicles to monitor apparatus locations within the geographical service area would improve efficiency of services provided by the governmental agency. Since many General Governmental field personnel are not assigned to vehicle related tasks, there is a need for a personal location device to track the location of an assigned individual in the event of an emergency and for routine management purposes. This tracking device may be incorporated within the voice communications equipment or be a separate personal device.

F. Land & Natural Resource Management

Organizations at local, state, and federal levels are charged with the specific oversight of our nation's environmental and agricultural resources. Activities of these organizations include management of forests, riparian environments, parks and various other environmental and agricultural resources for the common good of the general public.

The Land & Natural Resource Management mission is to serve the public through its activities directed to conserve, improve, and protect natural resources and environment. Communications needs are based on the performance of official duties. Major activities in the management of the fragile and limited public resources associated with forest, wildlife, fish, recreation, and other renewable resources include enforcement of environmental conservation laws; maintenance of air & water quality; hazardous, toxic, and solid waste management; mined land reclamation; wetland protection; environmental impact analysis; pesticide use regulation; fish & wildlife management; stream protection; park & primitive area management; and forestry.

Varied and wide area responses, including air support, require dynamic frequency assignments for all operational categories through well coordinated procedures. Land & Natural Resource Management systems require areas of operation covering entire states or regions.

Beyond the common requirements detailed in (A) above, Land & Natural Resource Management has the following unique requirements:

1. Land & Natural Resource Management Data Requirements.
 - a. Portable & Mobile Data Terminals. Mobile unit status and control provide essential cost and time saving abilities to day to day operations. Resource management and condition reporting are an essential component of large scale incidents such as wildland fires.
 - b. Data collection and monitoring. Public environmental resources such as water flow and quality provide instant information and warning freeing up personnel and equipment to perform their functions more efficiently. Infrastructure inventory and control can be transmitted as data allowing better control of required maintenance of resource support facilities.

- c. One Way Data Transmission/Telemetry. Data monitoring of fish and wildlife to allow better resource management.
 - d. Vehicle, Device and Wildlife Location Tracking. Location information allows more efficient use of equipment utilization, equipment management inventory and location control. The location and control of limited resources during routine and extended emergency incidents is crucial to safe and quick mitigation of such incidents.
 - e. Facilities Management. Facilities management includes oversight of bridges, buildings, and signs. Data transmission support assists infrastructure and repair through maintenance of inventory and status information. Also, resource identification requires survey information utilizing differential Global Positioning System (DGPS) accuracy. Accuracy for all of these requirements depends on the availability of DGPS. DGPS is provided by many means including transmission over dedicated public safety frequencies.
 - f. Wildfire Detection and Suppression. Data transport is required to support transmission of weather-related data and area vegetation and combustible materials inventory data.
 - g. Environmental and Waste Management Operations. Data transport is required to support transmission of data regarding water quality, well contamination and other data from remote monitoring or control systems.
2. Land & Natural Resource Management Video Requirements
- a. Real-time and close to real-time incident monitoring from remote sites (including airborne) provide up-to-date information on such incidents as wildland fires as well as crowd control in routine parks environments. Infrared real-time mapping from airborne platforms is rapidly becoming an essential component for fighting wildland fires.

G. *Land Transportation*

Organizations at local, state, and federal levels are charged with specific land transportation activities. These include maintenance and construction of transit railroads, highways, roads, bridges, and tunnels required to allow safe thoroughfare for the general public. These organizations also respond to events such as snow storms, mud slides, flooding, and hazardous material spills in order to allow safe passage on transportation infrastructures. Communications needs are based on official duties.

The transportation mission is to serve the public by establishing, operating and maintaining a high quality, cost-effective transportation system emphasizing safety, throughput and environmental preservation.

Many of the requirements for the Intelligent Transportation System (ITS) fall to the highway programs. These range from public information dissemination to monitoring transport vehicles regarding weight, height, and fuel permits. Innovative applications planned within these services may be unfamiliar to many in the public safety community especially those designed to aid in emergency vehicle response. ITS represents a broad range of applications that, because of their ability to enhance performance of different public safety communities' transportation and operations, apply horizontally across many other public safety communities' requirements. It should be noted that the operational requirements for ITS defined in this section of the report are derived from the ITS National Architecture and the user services on which the architecture is based. Many of the applications will enhance the safety of the individual traveler, and will be available to both personally owned vehicles as well as vehicles owned and operated by traditional public safety agencies. This creates an environment where spectrum use may be shared between public safety-related, public service and non-safety related functions.

The Intermodal Surface Transportation Efficiency Act (ISTEA) was passed by Congress and approved by the President in December 1991. It established the ITS program, which seeks to apply advanced communications and computer technologies to surface transportation systems in order to decrease traffic congestion, improve safety, reduce transportation related environmental impacts, and increase productivity. Public safety goals of the ISTEA legislation being addressed by ITS are reducing the frequency of accidents, reducing the severity of accidents, reducing congestion due to incidents, and enhancing traveler security.

In order to reduce the time and cost of implementing such a system, existing communications services will be used to the extent possible, provided they can meet ITS requirements. Some systems will require wireless data communications technologies (such as dedicated short-range communications using roadside readers and vehicular mounted transponders) or may require the use of collision avoidance radar. There are likely to be ITS-specific systems or applications requiring new spectrum. ITS may also require dedicated and shared use of frequencies currently allocated to public safety and other services.

A second component of Land Transportation is Public Mass Transit (i.e., trains and buses) that transports thousands of passengers each day. These organizations have direct responsibility for the safety and general welfare of their passengers during transportation. Emergency mass transportation incidents can arise as a result of human error, equipment failure, and environmental factors such as weather conditions. Operational needs to address these issues are incorporated in this section and represent operational concerns, system safety concerns, and the protection and maintenance of facilities and equipment. The need for communications is based on these safety and operational concerns and the need to provide the appropriate response to conditions as they arise. The majority of the operational requirements are based on the needs of major metropolitan areas where government is charged with providing these services, where massive numbers of people are transported daily, and services are essential to the general public.

Beyond the common requirements detailed in (A) above, Land Transportation has the following unique requirements:

1. Land Transportation Data Services
 - a. Infrastructure Inventory and Control. This information can be transmitted as data providing better control of required maintenance of structures such as bridges and signs.
 - b. Remote Public Information Systems. This includes changeable signs and traveler information radio systems, As well as weather and road condition data transfer from remote sites.
 - c. Road Maintenance Management. This includes managing bridges, buildings and signs, and road surface condition and repair needs inventory data acquisition. Road construction survey information requires differential Global Positioning System (DGPS) accuracy. Accuracy for all of these requirements depends on the availability of DGPS. DGPS is provided by many means, including transmission over dedicated public safety frequencies.

- d. Supervisory Control and Data Acquisition (SCADA). This includes monitoring systems and providing control functions to lighting, traffic control, pumping and specialized equipment such as toll collection and lane access control equipment.
 - e. Telemetry Systems. This includes the monitoring of infrastructure integrity such as pavement temperature, salt content, water flow and height at bridges, mud flow areas, and high wind areas to provide instant information and warning, thereby freeing up personnel and equipment to perform their functions more efficiently. The monitoring of equipment and fleet productivity increases effectiveness of operations.
 - f. Train Signal Data. A combination of on-board train data with information provided through an Intelligent Transportation System (ITS) suited to railroad operations is paramount in the avoidance of train collisions and improvement of system safety.
 - g. Vehicle and Device Location Tracking. Vehicle location information allows more efficient use of equipment, inventory management, and location control. Train locator systems can be used to ensure that trains carrying hundreds of passengers are not permitted to enter the zone of danger when emergencies ensue.
2. Land Transportation Video Requirements
- a. One-way video is required to view specific locations or interests through either snapshot, real-time or close to real-time accuracy to monitor traffic flow, facilitate incident response, and manage traffic control gates from remote sites.
 - b. Mass transit requirements are related to local operations, system safety and the property protection aspects of transit operations. One-way video provides a means to remotely view specific locations or interests through either snapshot or real-time video as necessary. For example, this feature allows crews to monitor safety within train cars in response to incidents or activation of passenger emergency alarms plus view upcoming stations and track for safety risks. Two-way portable video is necessary on a limited basis for

system or passenger safety when responding to a remote station. Field units and dispatch control points could communicate using real-time video with voice from mobile radios, hand held portables, or fixed sites.

3. Intelligent Transportation System (ITS) Requirements

a. The relationship between ITS and public safety has several aspects including: the safety of the traveler and the safety of public safety personnel performing mission related functions. Communications links will be required for point-to-point and point-to-multipoint control of subsystems. Public safety features of the Intelligent Transportation Systems network include:

- Emergency vehicle location tracking
- Emergency vehicle route guidance
- Emergency vehicle signal priority
- Driver and personal security
- Automatic collision notification
- Enroute driver information
- In-vehicle signing
- Incident detection and management
- Probe data for traffic control
- Transit management
- Priority treatment for transit
- Public travel security
- Automated roadside inspections
- Weight in motion
- Automated vehicle classification
- International border crossings
- Electronic clearance
- On-board safety monitoring
- Hazardous materials incident response
- Collision avoidance
- Intersection collision avoidance
- Safety readiness
- Pre-crash restraint deployment
- Automated highway system check-in
- Highway-rail intersection safety

b. Video requirements for Transportation management may include real-time situation updates from on-scene units to command centers. Multiple agencies may need to have the capability of monitoring another agency's video transmissions, however this capability must be controlled through a need to know or incident management process.

H. Federal Government & Department of Defense Operational Requirements

This section identifies operational requirements unique to federal government and Department of Defense public safety/public services agencies. The diversity and complexity of federal agency missions compel the use of a wide variety of telecommunications capabilities.

Effective and reliable radio communications are required for federal agencies and the Department of Defense to perform Congressionally mandated functions dealing with safety-of-life, security, and protection of federal property and military bases, protection of the President and other government dignitaries, enforcement of federal laws, protection of Native Americans, providing for enforcement of the Immigration and Nationality Act, operation of federal prisons, security of coasts and harbors, protection of natural resources, maintenance and protection of streams and inland waterways, distribution of water and natural resources, and many other essential missions.

To support these missions and responsibilities, federal and Department of Defense agencies frequently use wireless platforms, such as aeronautical and terrestrial-based mobile radio, HF, satellite, and cellular communications for clear and encrypted voice communications, paging, audio and video monitoring, alarm systems, electronic tags and tracers, technical surveillance, and limited data collection and transfer. These platforms are used both nationally and internationally, over diverse geographies, often requiring subscriber unit interoperability and the ability to communicate on a priority basis at all times.

From an aeronautical and terrestrial broadband wireless perspective, there are many similarities between federal uses and those of state and local governments. However, national security, extensive geographical coverage requirements, and privacy and security concerns are significant differences that require comment.

Beyond the common requirements detailed in (A) above, Federal Government & Department of Defense Operational Requirements have the following unique requirements:

1. Federal Law Enforcement Data Requirements

In order to provide compliance with legislative, executive, and departmental laws, orders and regulations, all federal use of wireless data must be protected with an appropriate level of cryptography. The wireless data requirements include such uses as mobile computing terminal applications, geographic position and automatic location data, emergency signals, transmission of reports, electronic messaging, home incarceration monitoring, and perimeter and vehicle alarms. In addition, multimedia systems employing both photographic and fingerprint transmission in conjunction with report automation must be supported. Remotely controlled radio devices are routinely used for turning off and on surveillance microphones, activating kill switches in vehicles, arming and disarming alarm and monitoring systems, and aiming video cameras. This control can be a one-time data burst or can be a continuous data stream.

- a. Sensors. Unattended border sensors/monitors, electronic agents, parolee monitoring and other remote sensing technologies will continue to evolve and will require increasingly sophisticated wireless communication paths.
- b. Encryption. Future information technology requirements for federal and Department of Defense law enforcement will include wireless multimedia data systems utilizing multiple types of encryption. In order to maximize the effectiveness of agents and officers in the field, a mobile office environment utilizing cryptographically protected wireless data communications must be developed.

2. Federal Law Enforcement Video Requirements

- a. Covert Video. Federal agencies are one of the largest users of covert video monitoring, particularly in dealing with organized crime and drug interdiction.

3. Fire, Natural Resources, and Public Service Data Requirements

These systems provide for the safety of the public and government personnel which includes over 300,000 postal vehicles and the security of 180 billion pieces of mail per year, monitoring and distribution of water, management of

timber growth and harvest, protection, operation, and management of our national parks, national forests, range and grass lands, wildlife refuges, protection of Native Americans and protection and management of their lands; forestry and range management; and assessment of mineral deposits.

- a. Hydrological Data. The gathering of hydrological data is crucial to assure the latest weather patterns, snow and precipitation levels, temperature and water quality are monitored in order to minimize a natural disaster due to these conditions. The emphasis is on the collection of data from remote sensors and prediction of flooding conditions based on that data. The Federal Hydrologic Program involves a large number of federal agencies as well as state and local agencies. The network, data, and frequency assets are shared among these agencies.
- b. Postal Services. Wireless data transmission is mission critical to the Postal Service in order to provide continued low cost mail service to over 95 million addresses.
- c. Seismic Monitoring. The gathering of seismic data is crucial to assure that earth movements and motions are cataloged and patterns detected to reduce potential earthquake damage, and potential loss of life and property.
- d. Wildlife Monitoring and Tracking. Data communications is required to protect endangered and threatened species and to control animal damage. These communications are performed with transmitters as small as dimes or as large as softballs. The gathering of wildlife data is crucial to track and catalogue the motions of specific species under study by multiple parties. The emphasis is on the identification of present and future migratory patterns that will influence the environmental habitats and future survival of these species.

4. Fire, Natural Resources, and Public Service Video Requirements

Requirements encompass a wide variety of scenarios ranging from provision of full-motion real-time video from on-site personnel or robotic sensors to remote command center, to slow-scan images for damage assessment. These video data should be accessible by a number of users under strict, need-to-know management procedures. Often a video image of current conditions is necessary to make critical decisions, like the release of water from a reservoir, in the management of natural resources.

- a. Hydrological Video. Hydrologic management requires the ability to transmit still photographs on demand to various locations to facilitate decisions concerning the adjustment of water releases or the evacuation of population downstream from a flood stage river.

5. Emergency Management and Disaster Services Data

The federal government provides an array of emergency and disaster response communications capabilities to protect the public and resources from natural and technological hazards. This involves a wide range of missions including prevention, mitigation, preparedness, response, and recovery. These services involve virtually every department and agency of the government. Where safety of life and property is at risk, communications systems that can operate reliably when normal systems are disrupted are essential. A significant number of the federal government emergency and disaster response communications systems interface (but are not necessarily interoperable) with state and local governments as well as with national volunteer organizations such as the Red Cross, amateur radio operators, and similar groups. Many specialized emergency requirements have unique spectrum-dependent needs that must also be satisfied by the nationwide dedication of radio spectrum for that purpose. As an example, federal and Department of Defense, state, and local government search and rescue teams deploying to the site of a national emergency or disaster need reliable communications to locate victims in collapsed buildings, administer medical and lifesaving treatment, and relocate them to safety or medical facilities.

In general, the data requirements of federal emergency management and disaster services are similar to those of their state and local counterparts. Often the data collected, analyzed, and disseminated in these services originates and terminates among federal, state and local agencies alike. A current example of federal emergency service data usage is the broadcast and response to Cospas-Sarsat distress alerts.

6. Emergency Management & Disaster Services Video Requirements

Like the data requirements, federal emergency management and disaster service video requirements are similar to those of their local and state counterparts

7. Transportation Data Requirements

Federal activities in aviation, maritime, highways, and railroads have a tremendous investment in both fixed and mobile operations. Federal and Department of Defense surface transportation operations provide a variety of management and oversight support to coordinate activities at various highway and rail sites.

Maritime safety and waterway management agencies within the federal government provide for the safe operation of the nation's navigable water resources. It requires coordination of many diverse, yet interrelated disciplines. From the inspection of user vessels and offshore facilities, to the provision of icebreaking capabilities to keep shipping routes open year-round, to ensuring port security, many tasks must be performed to ensure seamless utilization of coastal and inland waterways. In addition, safe passage is promoted through waterway management involving the interrelationship between vessels, waterway authorities, and facilities including docks, bridges, and piers

- a. ITS. The Intermodal Surface Transportation Efficiency Act (ISTEA) was passed by Congress and approved by the President in December 1991. The federal government manages the ITS program, as discussed above.
- b. Maritime Safety and Waterway Management. Examples of required services include: (1) short range aids to navigation, (2) acquisition of vessel position, identification, and sailing intentions, and (3) data dissemination with respect to ice conditions and/or port status.

8. Transportation Video Requirements

Video requirements for transportation management may include real-time situation updates from on-scene units to command centers. Multiple agencies may need to have the capability of monitoring another agency's video transmissions, however this capability must be controlled through a need to know or incident management process.

IV. Specific Project 25/34 User Requirements

The Project 25/34 standards that are developed in response to this SOR are intended to provide the base line technology standards for a nationwide high speed public safety data network. Whether the network is implemented as a series of individual networks or as one or more nationwide ubiquitous networks is outside the scope of this process. It is critical, however, that the ultimate standards envision total interoperability in all networks and at all levels, based on specified security and access limitations. Therefore, the following information will be used as requirements and guidelines in the standards development process and not as technical specifications.

- A. The SOR assumes the requirements contained herein may require modification as the wireless standards develop to accommodate new technologies.
- B. It is understood that certain technological and operational compromises may be required to fully complete the wireless standards as envisioned.
- C. Although the new wireless standards will provide direct interface to various local, state, and federal data platforms and applications, it is not expected that the standard will deal with network or protocol issues beyond that point.
- D. The proposed wireless standards are intended to provide interfaces that are transparent to both the wireless network and the network being interfaced.
- E. The wireless network end-to-end transit time should be less than 500 milliseconds.
- F. Wireless standards should be defined for interface to the following types of networks and protocols, to include:
 - Asynchronous Transfer Mode (ATM)
 - DS-1 and DS-3 rate network interfaces
 - Synchronous Optical Networks (fiber, infrared and laser) at the OC-1 and OC-3 rates
 - Frame Relay
 - Front End Processors (FEPs), as applicable
 - Basic Rate and Broadband Integrated Services Digital Network (ISDN) Networks
 - Microwave network interfaces
 - Public Switched Telephone Network (PSTN)
 - Satellite Communications Systems (SATCOM) interfaces.

- G. The wireless standards must, through dynamic partitioning of the network, provide for high speed simultaneous access to multiple networks or host computers by a single subscriber unit, as well as simultaneous access from multiple subscriber units to a single host.
- H. The wireless standards must support prioritization of access and routing, and allow for preemption. It is noted that ruthless preemption (defined as the immediate disconnection of a low priority user when a completely busy system is needed for high priority use) of non-public safety users on shared commercial/government systems is a policy issue that must be addressed as these systems are being planned.
- I. Wireless network access within the standardized system should be based on “first in - first out” (FIFO) within each priority class.
- J. The wireless network must support the transparent hand-off of subscriber units as they travel between fixed sites to minimize disruption of data transport.
- K. The wireless network must accommodate Type I, Type II, Type III and (if standardized and widely available) Type IV cryptographic algorithms with Over-the Air-Rekey (OTAR) consistent with Project 25 Phase 1 standards.
- L. The wireless network must accommodate Information Systems Security (INFOSEC) across the network such that security is an integral part of the enterprise solution. INFOSEC should include, but not be limited to, the following security disciplines: communications security (COMSEC), computer security (COMPUSEC), transmission security (TRANSEC), personnel security, administrative security, and operational security. INFOSEC is discussed in further detail in Appendix C.
- M. The wireless standards must include the ability to block access by unauthorized users.
- N. The wireless standards must provide for the distinct identification of all RF equipment and certain other components and features that may be required.
- O. The wireless standards must allow for the network to be developed, implemented, and managed on a “site-by-site” basis.
- P. The wireless standards must include the capability for remote, partitioned management of each network or site.
- Q. The wireless standards must allow the network manager to create an audit trail of all transactions that take place over the network.

- R. The network management system shall provide sufficient and easily accessible information to create statistical reports on network and subscriber traffic patterns and usage.
- S. The network management system must be capable creating agency-by-agency user reports and bills if necessary within the network or for any given site.
- T. The technology selected for Project 25/34 and the associated wireless standards should allow for dynamic information transfer rate by means of adaptive radio frequency modulation and error detection and correction coding and through the use of adaptive channel radio frequency bandwidth allocation.
- U. The technology selected for Project 25/34 must be capable of “graceful degradation” and/or complete redundancy when required.
- V. The technology selected for Project 25/34 must be capable of, and rated for, 100% duty cycle operation.
- W. All new technologies included in the proposed standard shall be bench tested before they are included in a final standards document; actual field testing of new technology prototypes is desirable.
- X. All standards that fulfill this SOR will be required to meet or exceed the Federal Bureau of Investigation’s (FBI) NCIC 2000 standards, as applicable at the time the wireless standards are approved.
- Y. The new wireless wideband data standards are intended to provide high speed access to the FBI’s Integrated Automated Fingerprint Information System (IAFIS) programs.

V. System and User Applications

This partial list of system and user applications have been included in the Project 25/34 SOR to establish a base line for standardized technology. 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. *General Requirements Applicable to All Applications*

- The wireless standards must support remote access to other public safety and general government reports.
- The wireless standards must support wideband network interfaces with host processors or switches managed by federal, state, county, and city agencies throughout the nation.
- The wireless standards should allow field subscriber units to access one of many host processors at a high data rate.
- The wireless standards should support the capability to implement direct user point of entry systems. Those systems will allow public safety and other government agencies direct, high-speed entry and access to critical government records from subscriber units.
- The wireless standards should allow access to public safety and general government client networks.
- The wireless standards should allow subscriber units to update multiple files simultaneously through the use of a robust network and switching standard.
- The wireless standards must include optional capabilities for robust subscriber unit and network security.
- The wireless standards should include the option of having a fully encrypted network, including control channels and password access codes if applicable.
- The wireless standards must support the capability for government agencies to transmit routine files from any subscriber unit to any other subscriber unit and/or a fixed base location.

- The wireless standards must support the capability for government agencies to transmit complex spreadsheets from any subscriber unit to any other subscriber unit and/or a fixed base location.
- The wireless standards must support the capability for government agencies to transmit electronic images from any subscriber unit to any other subscriber unit and/or a fixed base location. These images include suspect mug shots, photographs of missing persons, crime scene photos, Department of Motor Vehicle (DMV) license photos, photographs of articles of evidence, aerial photos of disaster scenes for damage assessment, photos of medical patient for remote diagnosis/triage, aerial infrared photos of fire scenes, and related photos of importance to government officials using the high-speed data network.
- The wireless standards must support the capability for government agencies to transmit graphical depictions of fires, accident scenes, natural disasters, chemical spills, structural data and other complex graphical information from any subscriber unit to any other subscriber unit and/or a fixed base location.
- The wireless standards must support the use of the GPS system, interconnected through the high-speed data network to locate specific public safety units in the field.
- The wireless standards must support the transmission of a combination of GPS information and graphical maps to identify specific locations of public safety concern.
- The wireless standards must support technology that will allow the field subscriber unit to access and transmit information that is magnetically stored on an individual drivers license or other type of personal identification. Although the standards are intended to allow for the transmission and reception of data from these cards, they are not at this time intended to include the card readers themselves.
- The wireless standards should include the capability of transmitting full motion or nearly full motion video from any subscriber unit to any other subscriber unit and/or a fixed base location. Examples include:
 - a) Vehicle pursuits
 - b) On site undercover surveillance
 - c) Medical didactic
 - d) Fire management
 - e) Hazardous material spill management (HAZMAT)

- f) Natural disaster site control
 - g) On scene criminal investigations
 - h) On-scene accident investigations
 - i) On-scene public disturbance control
 - j) On-scene bomb render safe or disruption procedures.
- The technologies selected for these wireless standards must support the transmission/reception of high-speed, wideband data at base stations, subscriber units, and through Radio Frequency (RF) repeaters.
 - The technology selected for these wireless standards should minimize RF network data routing and transport time to no more than 200 milliseconds.
 - The technology selected for these wireless standards should be capable of delayed transmission and/or remote store and forward when required.
 - The technology selected for these wireless standards should support full duplex or extremely fast response time to accommodate the implementation of “smart” systems that automatically update fields in files being transmitted from subscriber units with known information.
 - The technology selected for these wireless standards should be robust enough to allow for full duplex transmission and/or extremely fast response time to facilitate an almost instant identification of on-line data that appears to be in error and/or is inconsistent with pre-established protocol parameters.
 - The technology selected for these wireless standards should be capable of having sufficient bandwidth to allow for the automatic return to the subscriber unit of known file fields of personal information at the same time the public safety official is completing his/her report.

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

The wireless standards developed for Project 25/34 should:

- Allow for the remote transmission of and access to criminal justice incident reports.
- Allow for remote transmission of and access to standard uniform crime reports.

- Allow for remote transmission of and access to public safety traffic reports.
- Allow for the remote transmission of and access to criminal justice command and control information.
- Where possible, include the ability to provide a wireless subscriber unit with data terminal access to at least the following application platforms:
 - a) Computerized criminal history files
 - b) Disposition reporting systems individual wants and warrant files
 - c) Federal, state, county and city criminal case tracking files
 - d) Court/law enforcement and prosecutor case management files
 - e) Defendant voluntary assessment files
 - f) Correctional tracking files
 - g) Probation tracking files
- Support transparent, secure (authenticated and encrypted) access to the following types of local files:
 - a) National and local offender file
 - b) National and local victim file
 - c) Non-offender files as may be appropriate
 - d) Incident/complaint file as may be appropriate
 - e) National and local witness file
 - f) National and local apprehension file
 - g) Agency case files as appropriate
 - h) Agency and court disposition of charges files
- Support transparent, secure (authenticated and encrypted) access to NCIC and National Law Enforcement Telecommunications System (NLETS) files.
- Support transparent, secure (authenticated and encrypted) access to the following local, state and federal law enforcement files:
 - a) Wanted persons files
 - b) United States Secret Service Protective Service files
 - c) Foreign fugitive files
 - d) Unidentified person files
 - e) License plate files
 - f) Vehicle files
 - g) Boat files
 - h) Vehicle/boat parts files
 - i) Stolen article files

- j) Gun files and stolen gun files
 - k) Stolen and fraudulent securities files
 - l) Originating Agency Identifier (ORI) files
 - m) Interstate Identification Index (III) files
 - n) Convicted person and/or supervised release files
 - o) All available electronic image files
 - p) All authorized logically linked NCIC 2000 files
 - q) The existing and proposed "Enhanced" name and personal information files
 - r) The proposed improved NCIC identification files
 - s) Files available through the NCIC 2000
 - t) Files available through the Canadian Police Information Center Systems and the Canadian Department of Motor Vehicle (CDMV) databases
 - u) Access to Federal Corrections Systems (SENTRY) database files that are proposed under NCI 2000
 - v) Access to the proposed NCIC 2000 "Search and Reporting" systems
 - w) Access to the proposed NCIC 2000 on-line manuals and training programs
- Support transparent, secure (authenticated and encrypted) access to information systems (such as drivers license and vehicle registration files that are maintained at the state department of motor vehicles - DMV).
 - Support remote, secure (authenticated and encrypted) update of files kept for Uniform Crime Information systems.
 - Support secure (authenticated and encrypted) high-speed access to the FBI's NCIC 2000 image files directly from subscriber units in the field.
 - Support secure (authenticated and encrypted) high-speed access to the FBI's IAFIS files directly from a subscriber unit in the field.
 - Support secure (authenticated and encrypted) high-speed access to the FBI's proposed live ten-print scanner technology.
 - Support high-speed transmission of complete palm prints in less than 1 minute.
 - Support the rapid digital reproduction of motor vehicle drivers license pictures at a remote subscriber unit.

- Support the secure (authenticated and encrypted) rapid transmission of the FBI's NCIC 2000 image files directly to the subscriber units in the field on an approved basis.

C. Emergency Management & Disaster Services

The wireless standards developed for Project 25/34 should allow for remote transmission of, and access to:

- Emergency management incident reports.
- Emergency management information.
- Building floor plans, electrical plans and other structural data.
- Complex chemical information including formulas and containment plans.

D. Fire and Related Life & Property Protection Services

The wireless standards developed for Project 25/34 should allow for the remote transmission of, and access to:

- Fire and EMS incident reports.
- Fire management information.
- Building floor plans, electrical plans and other structural data.
- Complex chemical information including formulas and containment plans.
- On scene fire, emergency medical and related life and property protection command and control information.

E. General Government

F. Land and Natural Resource Management

G. Land Transportation

The wireless standards developed for Project 25/34 should allow for the remote transmission of, and access to:

- Highway, hydraulic and other types of engineering data.
- Highway safety reports.

H. Federal Government & Department of Defense