

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

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of

The 4.9 GHz Band Transferred from
Federal Government Use

)
)
)
)
)
)

WT Docket No. 00-32

CERTIFICATE OF SERVICE

I, David A. Williams, Senior Associate, Booz·Allen & Hamilton, Inc., 8283 Greensboro Drive, McLean, Virginia, 22102-3838, hereby certify that on this date I caused to be served, by first-class mail, postage prepaid (or by hand where noted) copies of the Federal Law Enforcement Wireless Users Group's 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), the original of which is filed herewith and upon the parties identified on the attached service list.

DATED at Fair Oaks, Virginia this 26th day of April 2000.



David A. Williams

SERVICE LIST

*The Honorable William E. Kennard, Chairman
Federal Communications Commission
445 12th St., SW, Rm. 8-B201
Washington, DC 20054

*The Honorable Harold Furchgott-Roth, Commissioner
Federal Communications Commission
445 12th St., SW, Rm. 8-A302
Washington, DC 20054

*The Honorable Susan Ness, Commissioner
Federal Communications Commission
445 12th St., SW, Rm. 8-B115
Washington, DC 20054

*The Honorable Michael Powell, Commissioner
Federal Communications Commission
445 12th St., SW, Rm. 8-A204
Washington, DC 20054

*The Honorable Gloria Tristani, Commissioner
Federal Communications Commission
445 12th St., SW, Rm. 8-C302
Washington, DC 20054

*Ari Fitzgerald, Legal Advisor
Office of Chairman Kennard
Federal Communications Commission
445 12th St., SW, Rm. 8-B201
Washington, DC 20054

*Paul E. Misener, Senior Legal Advisor
Office of Commissioner Furchgott-Roth
Federal Communications Commission
445 12th St., SW, Rm. 8-A302
Washington, DC 20054

*Daniel Connors, Legal Advisor
Office of Commissioner Ness
Federal Communications Commission
445 12th St., SW, Rm. 8-B115
Washington, DC 20054

*Peter A. Tenhula
Office of Commissioner Powell
Federal Communications Commission
445 12th St., SW, Rm. 8-A204
Washington, DC 20054

*Karen L. Gulick
Office of Commissioner Tristani
Federal Communications Commission
445 12th St., SW, Rm. 8-C302
Washington, DC 20054

*Thomas J. Sugrue, Chief
Wireless Telecommunications Bureau
Federal Communications Commission
445 12th St., SW, Rm. 3-C252
Washington, DC 20054

*Kathleen O'Brien-Ham, Deputy Chief
Wireless Telecommunications Bureau
Federal Communications Commission
445 12th St., SW, Rm. 3-C207
Washington, DC 20054

*James D. Schlichting, Deputy Chief
Wireless Telecommunications Bureau
Federal Communications Commission
445 12th St., SW, Rm. 3-C207
Washington, DC 20054

*D'Wana R. Terry, Chief
Public Safety & Private Wireless Division
Federal Communications Commission
445 12th St., SW, Rm. 4-C321
Washington, DC 20054

*Ramona Melson, Chief Legal Counsel
Public Safety & Private Wireless Division
Federal Communications Commission
445 12th St., SW, Rm. 4-C321
Washington, DC 20054

*Herb Zeiler
Public Safety & Private Wireless Division
Federal Communications Commission
445 12th St., SW, Rm. 4-C321
Washington, DC 20054

*Katherine Hosford
Public Safety & Private Wireless Division
Federal Communications Commission
445 12th St., SW, Rm. 4-C321
Washington, DC 20054

*Kris Monteith, Chief
Policy Division
Federal Communications Commission
445 12th St., SW, Rm. 3-C120
Washington, DC 20054

*Nancy, Boocker, Deputy Chief
Policy Division
Federal Communications Commission
445 12th St., SW, Rm. 3-C120
Washington, DC 20054

*Stan Wiggins
Policy Division
Federal Communications Commission
445 12th St., SW, Rm. 3-C120
Washington, DC 20054

*Ed Jacobs
Policy Division
Federal Communications Commission
445 12th St., SW, Rm. 3-C120
Washington, DC 20054

*Steve Weingarten, Chief
Commercial Wireless Division
Federal Communications Commission
445 12th St., SW, Rm. 4-C207
Washington, DC 20054

*Jeff Steinberg, Deputy Chief
Commercial Wireless Division
Federal Communications Commission
445 12th St., SW, Rm. 4-C207
Washington, DC 20054

Jeanne Kowalski, Deputy Chief
Public Safety & Private Wireless Division
Wireless Telecommunications Bureau
445 12th St., SW, Rm. 4-C324
Washington, DC 20054

International Transcription Services, Inc.
1231 20th St., NW
Washington, DC 20037

HAND DELIVERED