PUBLIC SAFETY
PSWN PROGRAM
WIRELESS NETWORK

Saving Lives and Property Through Improved Interoperability

Wireless Data Networking Standards Support Report

SUMMARY REPORT

FINAL

AUGUST 2001

TABLE OF CONTENTS

1. INTRODUCTION 1

1.1 Purpose 1
1.2 Background 1
1.3 Technology Progression 3
1.4 Document Organization 4

2. SUPPORTING ORGANIZATIONS 6

2.1 Association of Public Safety Communications Officials–International, Inc. 6
2.2 Electronic Industries Alliance 6
2.3 European Telecommunications Standards Institute 7
2.4 Telecommunications Industry Association 7

3. KEY INTEROPERABILITY AREAS 8

4. PROJECT MESA 9

4.1 Mobile Data 10
4.2 Background 10
4.3 Mobile Data User Requirements 11

5. CapWIN PROJECT 17

5.1 Intersections with PSWN Program 18

6. 3G TECHNOLOGY 19

ACRONYMS 22

1. INTRODUCTION

The Public Safety Wireless Network (PSWN) Program, a federally funded initiative jointly sponsored by the Department of Justice and the Department of the Treasury, is dedicated to improving safety by facilitating the implementation of interoperable communications among public safety organizations. Historically, voice radio communication has been the most common method used for both routine and emergency public safety communications; however, in today's environment, the use of computer-based mobile data information systems has become increasingly important to the effective delivery of public safety services. Because common wireless data networking standards have not been established, the public safety community must now address interoperability issues associated with data communications. Disparate information systems are being used and regularly being implemented at the local, state, and federal levels. Therefore, it is now incumbent on the public safety community to explore wireless data communications alternatives capable of interconnecting multiple computer systems and delivering critical (non-voice) information to the field.

In the long term, commonality for wireless data standards will provide the public safety community with information-sharing opportunities not currently available (e.g., graphics or video-based applications). Further, standards-based wireless data technology will mitigate compatibility issues associated with proprietary technology, thus supporting a faster technology transition for users and allowing agencies to avoid costly protocol conversion and system interfacing measures. The PSWN Program is in a position to leverage the lessons learned from the evolution of voice technology and apply these lessons appropriately to the data communications arena. By participating in the development of wireless data standards, the PSWN Program will facilitate the effective transfer of information and the ability of the public safety community to provide a more rapid and appropriate response to support the public at large.

1.1 Purpose

The purpose of the Wireless Data Networking Standards Support Report is to identify the progress made in the development of wireless data standards as they relate to the Project MESA (Mobility for Emergency and Safety Applications) and Capital Wireless Integrated Network (CapWIN) efforts, as well as with associated technology advancements (e.g., third-generation [3G] technology). Because of the significant impact of wireless data technology on administrative, operational, and interoperable communications for public safety users, the PSWN Program is monitoring these developments to provide a single point of reference outlining relevant data standards development activities ongoing in the public safety community.

1.2 Background

Originally, public safety agencies had few options in acquiring mobile data technology systems other than different infrastructure providers. The agencies were required to implement a government owned and operated private-data radio network, which in most cases was used exclusively to support a single agency or department.

Private data radio infrastructures provide a dedicated network tailored to the specific needs of a particular public safety agency. This approach requires an agency or jurisdiction to construct and operate its own wireless data network infrastructure, taking responsibility for licensing, implementation, funding, operations, and maintenance of the infrastructure and devices.

Mobile data applications and mobile data devices are typically implemented at the same time during the acquisition of a private data radio network. Some system integration, however, is usually required to implement specific mobile data applications, such as computer-aided dispatch (CAD) system interface, records management system (RMS) interface, and state/National Crime Information Center (NCIC) interfaces. Data warehouses, containing information to be utilized by law enforcement, fire, and EMS agencies, must be populated and made accessible to appropriate inquiries.

Currently, private data radio networks can provide up to 25,600 bits per second (bps) data throughput per channel, which is usually sufficient for most text-based public-safety applications. These solutions are designed to be secure and provide priority access to public safety users. Private data radio networks have a proven record of accomplishment in the public safety community safety.

Today, private data networks remain a viable solution for both public safety and non-public safety agencies and may be constructed for multiple agencies, organizations, or jurisdictions, while providing data communications coverage over wide areas. The sharing of these solutions among agencies with different missions appears to be a less costly solution, with greater coverage opportunities, and a higher degree of information resources access than standalone systems.

Public safety agencies also have the option of leasing wireless data network infrastructure and services from a variety of providers, much as an agency would acquire telephone or wired networks and services from a local telephone company. Commercial mobile data networks provide wireless data access to a variety of subscribers in various organizations, including government agencies. These commercial networks, offered by specialized mobile radio (SMR) and enhanced specialized mobile radio (ESMR) providers, use a variety of communication technologies, including spread spectrum, cellular digital packet data (CDPD), and satellite mobile data. Each relies on a terrestrial network for connectivity with host networks and computers.

By using commercial wireless networks, public safety agencies can avoid investing significant cost and time in constructing a fixed, private infrastructure that usually accounts for 40 to 60 percent of the total, one-time costs of a wireless data system. Use of commercial wireless networks, however, may entail significant monthly subscriber fees per user device. These recurring costs typically lead to higher system life-cycle costs but can sometimes be mitigated through alternative purchasing agreements or cooperative purchasing vehicles.

Many of the available commercial wireless networks employ open protocols and support a variety of mobile user devices. Often, these networks are easily scalable to allow expansion to

maintain acceptable data communication rates. Nevertheless, significant systems integration is usually required to develop interfaces among applications, such as CAD/RMS, and between the wired network infrastructure and the commercial wireless network. Security of these connections and state/NCIC system connections also becomes a significant integration issue when using commercial networks.

A distinct advantage of commercial wireless networks is the increased bandwidth and data throughput they may provide (up to 28,800 bps throughput per channel). Because commercial networks typically have more sites and channels than a private data radio system, the design of commercial networks allows more users to gain access at these higher speeds. A potential disadvantage is that the commercial network may be shared among many users and during periods of high demand, potentially causing public safety users to experience delays in transactions. These delays may not be acceptable for mission-critical applications. Several of the commercial vendors mitigate this deficiency by reserving specific frequency resources per site for public safety subscribers within their networks.

Due to the limited deployment of commercial networks in rural areas, coverage disparities often exist. Commercial network providers are generally reluctant to commit to less populated regions unless a guaranteed subscriber base is present to support network infrastructure costs. As a result, coverage limitations may also be unacceptable for mission-critical applications. Thus, agencies contemplating the use of commercial networks for mission-critical applications should seek contractual guarantees of access and availability.

As technology continues to evolve and higher bandwidths are required to support data-intensive applications, such as mapping, digital mug shots, and automated fingerprint identification, commercial networks may be more easily adaptable to support these requirements. Some public safety agencies have opted to use a combination of private and commercial systems to support operational requirements and to ensure that mission-critical transactions are expedited through a private data radio system while data rate intensive applications are directed to commercial network connections.

The opportunity to develop multiagency, multijurisdictional systems has also expanded in recent years. Many public safety agencies in the same geographic area are deploying shared system solutions while maintaining agency autonomy on a shared infrastructure. These shared solutions provide a lower initial cost, as well as extended coverage areas to each participating agency, and are accomplished using advanced network control processors and message switching technologies. In this type of configuration, multiple message switches, which connect to different agency infrastructure systems, are connected to the private data radio system. Through application development for the message switches and the mobile data devices, interconnection of various agency systems may be extended to all field resources supported on the network.

1.3 Technology Progression

Since the late 1970s, the public safety community has been at the forefront in the use of wireless data capabilities. As technology has evolved, so have the capabilities and the alternatives for wireless data transmissions. Public safety agencies, as “early adopters” of

wireless data technologies, have benefited from the progression and development of many new and innovative concepts that have been provided as extensions of existing information technologies already deployed to the field.

Initially, mobile data systems were used primarily by law enforcement to extend state and national criminal database access to the officer in the field. Unit-to-unit messaging was also a standard capability. As public safety agencies further embraced information technology with the deployment of CAD systems and then RMS, additional mobile data requirements were developed and have been extended to all facets of public safety services. In addition, agencies began to recognize the opportunity to use mobile data technologies to effectively supplement voice communications and relieve congestion on voice frequencies, especially in large urban areas where additional frequencies are not readily available. Despite the rapid evolution of wireless data technology, problems are mounting because of insufficient data speeds to support the operational requirements and the feature-rich applications favored by today's public safety community.

1.4 Document Organization

The Wireless Data Standards Compilation Report is divided into the following four sections:

- **Summary Report.** The summary report provides an overview of the status of wireless data standards through the activities of two key projects, Project MESA and CapWIN. In addition, a brief outline of organizations central to the development of wireless data standards is also provided. The key areas of interoperability, as they intersect with wireless data standards, are also featured in this report. A synopsis of mobile data requirements collected from public safety agencies and the public safety vendor community is also included to emphasize the need for mobile data standards to better support the myriad applications required by today's public safety organizations. (Note: This information was derived from public safety agencies, procurement documents issued by agencies for mobile data systems, and ongoing mobile data development efforts discussed by the public safety vendor community.) Finally, this report summarizes the current wireless data standards associated with 3G technologies.

- **Appendix A—Project MESA.** As the first international organization specifically addressing wireless data standards, Project MESA is in a position to encourage the development of standards that benefit the Public Protection and Disaster Relief Sectors worldwide. This appendix includes the meeting notes, reports, and efforts of this partnership dating from project inception through June 2001. A Statement of Requirements for mobile data, originally drafted by a combined effort of the Project 25 and the Project 34 Committees, New Technology Standard Project, is included.

- **Appendix B—Capital Wireless Integrated Network (CapWIN).** A cooperative effort between the states of Maryland and Virginia, and the District of Columbia, the CapWIN project is developing the roadmap for the wireless standards-based transfer of information, primarily data, for public safety and transportation organizations. This appendix contains the documentation developed as a result of the project's initial efforts.

- **Appendix C—Third-Generation (3G) Technology.** 3G technology includes the commercial standards for the next generation of cellular technology, which is positioned to provide convergence with Internet technologies. This appendix is a compilation of information and reports that describe the current 3G activities related to wireless data standards.

2. SUPPORTING ORGANIZATIONS

Several associations and organizations have been recognized by the public safety community for their continuing efforts in the development of wireless data standards. Four predominant organizations are featured in this section: Association of Public Safety Communications Officials–International, Inc. (APCO), Electronic Industries Alliance (EIA), European Telecommunications Standards Institute (ETSI), and the Telecommunications Industry Association (TIA). Due to the valuable services and thought leadership that each provide for the public safety community, these organizations have become leaders in this arena. Other organizations are involved in the development of wireless data standards, but their efforts are generally not directed by the needs of public safety.

2.1 Association of Public Safety Communications Officials–International, Inc.

APCO is among the first national-level organizations committed to improving public safety communications. It is a large, non-profit organization with more than 15,000 members from various segments of the international public safety community including fire, law enforcement, emergency medical services (EMS), and transportation agencies. One of the primary missions the association supports is to "foster the development and progress of public safety communications and supporting information technologies by means of research, planning, coordination, training, and education." To accomplish this mission, APCO establishes "projects" for the development of protocols and standards within a related technology focus area.

APCO, the National Association of State Telecommunications Directors (NASTD), and several federal agencies, initiated Project 34 (P34). P34 is a project critical to improving public safety interoperability and promoting market competition among wireless data vendors. However, APCO is no longer the oversight organization for this project. The project has been passed to a new organization, Project MESA, and renamed the same. For additional information regarding APCO activities, please refer to www.apco911.org.

2.2 Electronic Industries Alliance

The EIA is the outgrowth from an alliance of six previously existing associations: TIA, Consumer Electronics Association (CEA), Electronic Components, Assemblies and Materials Association (ECA), Government Electronics and Information Technology Association (GEIA), JEDEC—Solid State Technology Association, and Electronic Industries Foundation (EIF). While each of these associations is a leader in its respective industry, when combined, a cross-sector, high technology partnership was formed.

EIA is involved in numerous activities, such as trade shows, seminars, and conferences. In addition, EIA leadership provides technical expertise on issues such as encryption, FCC reform, and globalization for private companies. EIA established a Government Relations Department, which is composed of several councils, to participate in legislative and regulatory advocacy for the U.S. electronics industry. In fact, EIA has developed over 4,000 industry standards. These endeavors signify EIA's role as an important organization in the development

of technical standards. For additional information regarding EIA activities, please refer to www.eia.org.

2.3 European Telecommunications Standards Institute

Dating back to 1998, ETSI has been recognized internationally as a leader in establishing electronic communications standards. More than 800 members and observers from 52 countries support the organization's mission "to produce the telecommunications standards that will be used for decades to come throughout Europe and beyond." In fact, ETSI addresses any European organization's interest in telecommunications standards.

The European market determines and prioritizes ETSI's standards work program. Thus far, numerous key areas for wireless standards have been identified, including Internet telephony, terrestrial trunked radio (TETRA), and maritime radio. Within the work program, research and the resulting documentation are being accomplished simultaneously for several technology issues on an ongoing basis. It is important to note that the standards established by ETSI are initially voluntary. In the future, some may be adopted as a technical base for a directive or regulation. Additional information regarding ETSI efforts are detailed at www.etsi.org.

2.4 Telecommunications Industry Association

TIA, a trade association in the communications and information technology industry, is a principal sponsor of trade shows, domestic and internal advocacy, and standards development. Formed as the result of several association mergers in 1988, TIA provides a market-focused opportunity for more than 1,100 member companies to further their respective business positions and economic potential.

The organization is structured into five divisions—User Premises Equipment, Network Equipment, Wireless Communications, Fiber Optics, and Satellite Communications. This structure is used to maximize membership benefits by segmenting the focus of the various communications technologies. Voluntary industry standards are then generated that support U.S. interests in communications products and systems. For further information concerning TIA activities, refer to www.tiaonline.org.

3. KEY INTEROPERABILITY AREAS

As a supporter of wireless data standards development, the PSWN Program promotes new opportunities for improved interoperability. The development of wireless data standards is expected to encourage more widespread use of wireless data communications within the public safety community, thus creating another medium for the exchange of information. To advance this objective, the program has identified focus activities to support wireless data standards within the five key issue areas of interoperability. Table 1 lists these key interoperability issue areas, and the associated focus activities, as they intersect with wireless data standards.

Table 1
Key Interoperability Areas and the Intersections with Wireless Data Standards Activities

Interoperability Issue Area	Wireless Data Standards Activities
Coordination and Partnerships	• Support CapWIN and Project MESA activities • Leverage lessons learned from voice technology progression • Promote the creation of wide-area, regional or statewide systems to support mobile data communications for multiple agencies
Funding	• Promote vendor competition—resulting in lower costs for equipment and services • Leverage agency investments in technology to minimize premature replacements and facilitate smooth migration to new technology
Spectrum	• Encourage efficient use of limited spectrum available for data communications • Promote application of new technologies to maximize available frequency usage
Standards and Technology	• Ensure timely and accurate dissemination of information • Promote use of mobile data technology for public safety activities • Open additional avenues for information resource sharing and encourage the efficient use of limited spectrum available for data communications
Security	• Facilitate widespread implementation of network security • Promote implementation of advanced encryption standards to protect user information

4. PROJECT MESA

On February 5, 2001, in Mesa, Arizona, two of the world's leading standards development organizations (SDO), ETSI and TIA, finalized the Public Safety Partnership Project Agreement. This landmark partnership agreement, now named Project MESA, in recognition of the city where it was finalized, establishes a collaborative project to produce a broadband mobile data communications standard specifically for public protection and disaster relief organizations.

Project MESA represents the first international standards development partnership and encourages direct involvement of public safety and public protection users, their organizations, and industry representatives. This involvement will assist in creating applicable standards that will permit operationally accurate implementations of the relevant communications technologies. Specifically, the Project MESA concentration is on developing broadband mobile data standards (data transmission rates of 2 megabits per second [Mbps] or greater).

The organizational partners, participating agencies, and industry representatives of Project MESA recognize the continuing need and growing demand for broadband mobile data communications standards within the law enforcement, fire suppression, EMS, other public protection agencies and military peacekeeping organizations. Public safety's interest in this project continues to be driven by the emergence of greater overall technology capabilities supporting the criminal element that far outstrip those of public safety and protection organizations. Figure 1 illustrates Project MESA's organizational structure.

Figure 1
Project Mesa

The objectives of Project MESA are to establish standards and specifications for broadband mobile communications technology for the wireless transport and distribution of rate-intensive data, digital video, and voice for both discipline-specific and general public safety applications. Project MESA will also concentrate efforts on increasing air interface rates beyond the currently available standards. For further information concerning Project MESA activities, refer to www.projectmesa.org.

The broadband mobile data standards and specifications that are the focus of Project MESA are contemplated to meet or exceed the present day standards and support a variety of public safety applications. These applications may include the enhancement of present-generation inquiry and reporting capabilities; the expanded use of video, imagery, and telemetry; and new opportunities for wireless and remote robotics command and control.

4.1 Mobile Data

Mobile data provides a means for incident responders to remotely access information-system-based data. It offers the means to access routinely used databases, such as those needed to check for wanted or missing persons, driver's and vehicle license information, and NCIC-related information, without the delay associated with requesting a voice relay of the required information.

The wireless technology supporting mobile data has been available since the mid-1970s but has evolved from mobile status terminals (MST) capable of only simple status messaging, to mobile data terminals (MDT) capable of basic queries, to present-day mobile data computers (MDC) capable of the full feature sets available on any laptop computer. Public safety agencies have also embraced wireless data capabilities using handheld devices. As the technology continues to evolve and becomes more widely used, it becomes ever more important to identify a basic set of user requirements to which vendors can design systems, applications, and devices, and to identify standards for these mobile data systems that will improve usability and interoperability among data users.

4.2 Background

When discussing mobile data, it is important to differentiate between mobile data and mobile computing. Mobile computing means that a handheld, portable, or vehicle-mounted computer is used to gather the information. Later, this collected information may be transferred from the mobile data device via floppy disk, RAM card, or other media, or potentially through a connection to a wired local area network (LAN). Conversely, a true mobile data solution uses a handheld, portable, or vehicle-mounted computer to gather the information, which is then wirelessly transferred to the network without a physical connection or use of an intermediate storage media.

The primary difference, beyond cost, is the need or desire for the real-time transfer of the collected information. In the case of field-generated reports requiring interaction with other public safety staff, a greater need for the real-time delivery may exist. A report designed only to document a service for records purposes might not require the immediacy of a wireless transfer.

In many cases, public safety mobile data solutions may incorporate elements of both mobile computing and mobile data, depending on an agency's needs. The emergence of faster and more capable transport media for data communications will continue to blur this distinction, and, in the future, the delayed transfer of information may not be required or will be substantially minimized.

4.3 Mobile Data User Requirements

Based on input from various public safety user agencies and members of the public safety vendor community who specialize in the development of technology systems, the following is a synopsis of major features, functionality, and capabilities desired by many public safety and public protection organizations:

- Database access
- Biometric sampling
- Digital photography and imagery
- Real-time video
- In-vehicle navigation
- In-vehicle mapping
- In-vehicle printing
- Electronic messaging
- Mail system access
- Scanning
- Automatic vehicle location support
- Text-to-voice capability
- Voice recognition
- Computer-aided dispatch
- Records management systems
- Field reporting
- External database connectivity.

Many of these capabilities are available in present vendor offerings. Some of these applications and features are available with limited scope or are in pilot environments and may be further enhanced by new or emerging mobile data technologies. Listed below is a more detailed description of each requirement.

1. Requirement—Access to State and National Criminal Information Systems.

Description—Law enforcement agencies rely heavily on the ability to access the various criminal information systems from the field. The application should allow "smart inquiry forms" that submit transactions to the various connected systems based on the information entered into the forms. Supported inquires through state telecommunications, NCIC, and the National Law Enforcement Telecommunications Systems (NLETS) should include—

- Wanted/missing persons
- Stolen vehicles
- Stolen articles
- Stolen guns
- Stolen boats
- Stolen license plates
- Driver's license information
- Vehicle registration information
- NCIC 2000 enhanced systems[1]
- State and NCIC III[2] criminal history information
- National Sheriff's Association HazMat/Chemical Database.

[1] NCIC 2000 provides all the services of the original NCIC system, in addition to new technology features, including mug shot, fingerprint data, and image storage and retrieval technology.

[2] NCIC III is the criminal history component of the NCIC system. Triple "I" stands for the Interstate Identification Index, which is a compilation of criminal history records submitted to NCIC from participating states.

2. Requirement—Support for Biometric Sample Collection Devices

Description—This capability will provide a wired or wireless connection to the mobile data device that will enable the use of a device capable of collecting biometric samples. This capability may include support for fingerprint scanners used in NCIC 2000 wanted person identifications. The capability should also support other devices such as retinal scanners or (future) portable facial recognition scanning devices. Potentially, EMS agencies could use this technology to further patient data collection efforts using non-invasive techniques.

3. Requirement—Digital Photography and Imagery Support

Description—The mobile data device (MDD) should permit connection of digital cameras to allow download, upload, and wireless transmission of pictures. The MDD should also be capable of retrieving digital images from local, state, and federal image systems depicting mug shots of individuals or images, specific to an incident or offense.

4. Requirement—Real-Time Video Reception and Transmissions

Description—Public safety agencies indicate the ability to transmit and receive real-time video is desired. This capability would permit authorized fixed or mobile users to access real-time or near-real-time video feeds from—

- Airborne video units
- Highway traffic cameras
- Surveillance cameras at incident locations
- Vehicle-mounted video units
- Handheld video devices (to include helmet mounted units, as those used in fire and rescue operations)
- Robotic devices.

EMS agencies specifically desire support of real-time video transmissions to and from the hospital or medical direction sources.

5. Requirement—In-Vehicle Navigation

Description—Public safety agencies desire to effectively use vast geographic information systems (GIS) resources that provide very detailed mapping of service areas and surrounding areas. Agencies desire in-vehicle mapping and "best-route" navigation from a present position to a pending incident using graphical representations of resources deployed to the field.

6. Requirement—In-Vehicle Mapping

Description—This function provides the ability to interactively map location-based information from wirelessly connected host systems. These systems could include any

information systems supporting address or coordinate-based location data. Specifically the mapping systems should provide—

- Analysis and presentation capabilities
- "Pin-mapping" of incidents or activities
- Proximity of hazardous locations to a dispatched location
- Recent aerial photography of an incident location
- Street network and road closure information
- Building or structural outlines
- Topographic representations.

7. Requirement—In-Vehicle Printing

Description—Agencies desire the ability to print reports or other information in the vehicle. A ruggedized and reliable mobile printing device is required. This capability should provide for printing—

- Citations
- Fire inspection reports
- Barcodes
- EMS patient reports
- Signature documents
- Imagery such as "line-ups" of mug shots or driver's license photographs.

8. Requirement—Real-Time Electronic Messaging

Description—Agencies require real-time messaging that provides immediate message delivery and receipt confirmation. The messaging application should provide—

- Device-to-device(s) messaging
- Device-to-message group(s)
- Messaging with a dispatcher(s)
- Broadcast messaging
- Prioritize messaging
- Emergency messaging.

9. Requirement—Access to Agency Electronic Mail Systems

Description—This function should provide e-mail, possibly with attachments, to support normal administrative messaging and file transfers. Access to agency e-mail servers, and potentially to the Internet e-mail, should be supported.

10. Requirement—Device Support for Magnetic Stripe, Barcode, and Indicia Scanning

Description—Wireless devices should support scanning components to access information contained on magnetic stripes, barcodes, and indicia. The mobile device applications should permit the incorporation of the scanned information into device-

resident applications for additional transactions such as local, state, and NCIC checks or completion of various reports generated by EMS, fire, or law enforcement personnel.

11. Requirement—Support for Automatic Vehicle/Officer Location Information

Description—Automatic vehicle location (AVL) and automatic officer location (AOL) should be integrated with the mobile data devices and supported infrastructure systems. The positional information from the AVL/AOL system should be used by other support systems, such as CAD, to enhance and expedite resource responses and assignments, and could support proximity-based CAD status changes when an assigned resource reaches an incident location. Incorporating AVL/AOL and GIS capabilities that will precisely identify a resource and call for service location should allow the CAD system to automatically dispatch calls for services to field resources with limited dispatcher intervention.

12. Requirement—Device Support for Text-to-Voice Capabilities

Description—Agencies indicate that the ability of the wireless data device to convert textual information to audible voice is beneficial. The capability allows personnel to continue vehicular operations while information received is "read" to them.

13. Requirement—Support of Voice Recognition Technology

Description—Agencies believe that emerging voice recognition technology should allow the "hands-free" operation of a mobile data device and resident applications through voice commands. Furthermore, field report completion should also be supported to eliminate or minimize typing. Wireless headsets should be incorporated to support voice recognition technologies and voice radio operation potentially enabled through Bluetooth[3] or other personal area network (PAN) technology potentially in (4.9 gigahertz [GHz])[4].

14. Requirement—Computer-Aided Dispatching System Integration

Description—Many public safety agencies employ CAD systems and believe that their integration with mobile data technologies can enhance and expedite service provision. Integration of CAD systems with mobile data devices should provide the following capabilities:

- Access to real-time unit status and incident information
- Non-voice communication of calls for service information

[3] Bluetooth refers to a short-range wireless technology designed to simplify communications among network devices and between devices and the Internet. It also aims to simplify data synchronization between network devices and other computers. Bluetooth operates on unlicensed spectrum in the 2.5 GHz range and may be used to establish a PAN.

[4] 4.9 GHz is an area of radio spectrum that several vendors believe may be well suited to support public safety communications networks. PAN industry representatives indicate concern regarding the use of Bluetooth because it is unlicensed and shares a rather "crowded" area of spectrum that has a high potential for interference.

- Electronic updating of resource status
- Access to location contact information, warnings, hazards, fire pre-plans, hydrant information and knox-box[5] locations
- Non-voice message acknowledgements
- Electronic status changes and updates
- Historical information regarding previous calls to locations
- Personnel workload statistics
- Unit/incident histories
- Beat/area activity reviews
- Proximal information alerts
- Minimizing of voice radio traffic upon congested frequencies.

15. Requirement—Records Management Systems Integration

Description—Many public safety agencies desire full access to their existing RMSs. The intent is to provide the same levels of accessibility through wireless connections in the field as are provided through wired connections. All disciplines of public safety agencies indicate requirements to have comprehensive and sophisticated opportunities for inquiry, retrieval, and analysis of their RMS information in the field

Furthermore, law enforcement agencies desire comprehensive RMS inquiry transactions that are coupled with state and NCIC and NLETS system inquiries negating multiple input transactions.

16. Requirement—Wireless Field Report Completion and Submission

Description—The capability to submit report information from a mobile data device has long been a desire of many public safety agencies. Field reporting applications should support pre-population of reporting form fields with information that has been previously collected from the CAD systems or other system inquiries. Information obtained through magnetic stripe and/or bar code readers should be transposed to reporting or inquiry query transaction forms.

The ability to capture electronic signatures should be provided for field reports requiring signatures such as citations, offense reports or EMS patient refusal forms. Field reporting should support submission, review, and retrieval of departmental reporting forms.

17. Requirement—External Systems Information On-Demand

Description—Public safety agencies have expressed the desire for connectivity (for querying purposes only) to the following types of systems:

5 Knox-boxes are secured harden storage containers found primarily on the outside of commercial structures that contain building keys, access cards, floor plans or other important information that may be vital to responding public safety agencies. Responders carry a master key to obtain access to the Knox-box.

- Tax assessors systems
- Voter registration systems
- Judicial systems—local, county, state—criminal and civil
- Jail systems—local, county, state
- Probation and parole management systems
- Utility company systems—water, power, gas
- Sex crimes registry databases
- Local, county, state imagery databases
- Code/building inspections department systems
- Poison control agencies
- Environmental control agencies
- Geographic information systems
- Regional crime information/crime analysis systems.

5. CapWIN PROJECT

An important partnership was formed when the Capital Wireless Integrated Network (CapWIN) project leaders extended an invitation to the management of the PSWN Program to support this significant interoperability project. Through their collaborative efforts, new opportunities for sharing available resources, when appropriate, will be realized by the regional public safety and transportation communities. The CapWIN project mission is "to ensure a coordinated response to any transportation, natural disaster, or public safety incident in the Washington, DC, region." Through the partnership efforts of the states of Maryland and Virginia, and the District of Columbia, the CapWIN project supports the development of an integrated transportation and public safety wireless data network. To be used by the regions public safety and transportation organizations, this network is intended to integrate data communications through an interconnection of the participating agencies' existing wireless data systems. As a result, the expansion of available information assets and the proficient exchange and dissemination of information will be provided to incident responders when completing day-to-day activities or responding to critical multijurisdictional incidents. This data includes access to "hot files" in adjoining states and other critical information that could save lives.

The CapWIN project is intended to be accomplished in three phases that span three years. The first phase includes a data-gathering effort, along with an analysis of user requirements. The data-gathering effort resulted in the development of the *Best Practices White Paper: Transportation Management and Public Safety Integration* and *Study of Best Practices in Information Integration Projects*. Based on the requirements analysis, *An Assessment of Select Metropolitan Washington Public Safety and Transportation Agencies Users Needs* was produced. These efforts culminated in the *Capital Wireless Integrated Strategic Plan 2001*. In conjunction with the development of these documents, a CapWIN proof-of-concept pilot was initiated. The pilot test targets multiple agencies sharing many varied information systems and provides system interconnection via the CapWIN pilot test system.

The current CapWIN focus is Phase 2, during which efforts will be made to add functionality and expand the system. This phase will be completed using a multiyear phased implementation approach that began with the issuance of a Request for Proposals (RFP). The RFP, provided for reference, as Volume III of this report, solicits vendors to propose a solution for providing data communications for agenciess without mobile data service and interconnection among existing wireless data systems and the various criminal justice, law enforcement, fire and EMS services, and transportation databases. The proposed solution should permit real-time messaging between dissimilar mobile data systems and enable field units, regardless of service type or jurisdiction, to access internal information systems used by the various participating public safety and transportation agencies. The proposed solution should also support state and national law enforcement telecommunications systems and crime information centers. Vendor responses to the RFP were due in July 2001. The PSWN Program has begun assisting in the comprehensive evaluation of the proposed technologies. To support agency participation, a business plan is under development to identify strategies where costs and resources can be shared and the overall investments of agencies can be reduced.

Phase 3 efforts are not definitive but will likely focus on additional system enhancements and further system expansion. Future network expansion will target interfaces to local databases including computer aided dispatch applications. Research efforts will be ongoing, and to provide the information necessary for project replication, a model will be developed that includes formal documentation.

The CapWIN project has numerous supporters, including the Maryland State Highway Administration; Virginia Department of Transportation; U.S. Department of Transportation; National Institute of Justice, Office of Science and Technology; and the PSWN Program. Through the support of these agencies and the transportation and public safety communities, the CapWIN project will be the first multistate, public safety and transportation integrated wireless data network.

5.1 Intersections with PSWN Program

The PSWN Program and CapWIN project are partnering to improve interoperability for voice and data communications, respectively. Through the technical expertise and forward leadership of both organizations, the public safety community is presented with new approaches to increased opportunities for interoperability. The CapWIN activities support the interoperability issue areas identified by the PSWN Program. As shown in Table 2, the intersection of key PSWN Program interoperability issue areas are presented with the CapWIN project activities.

Table 2
Key Interoperability Areas and the Intersections with CapWIN Activities

Interoperability Issue Areas	CapWIN Efforts
Coordination and Partnerships	• Support coordination and partnerships efforts for multiple agencies at the local, state, and federal levels
Funding	• Identify and leverage multiple funding sources
Spectrum	• Identify and recommend efficient utilization of spectrum for regional government services
Standards and Technology	• Define standards to ensure applications security
Security	• Establish security requirements for wireless data

6. 3G TECHNOLOGY

In 2000, the International Telecommunication Union finalized the specification development of the next generation of mobile communications technology. This next-generation technology, designated 3G, promised increased data rates above those available in first-generation (i.e., analog cellular) and second-generation (i.e., personal communications services [PCS]). The specification also covers what 3G technology will be used for, with allocations for common billing and user profiles across different carriers, and support of multimedia services such as bandwidth on demand, mail storage, and call forwarding. 3G digital cellular technology promises increased bandwidths of up to 384 kilobits per second (Kbps) for street level for pedestrian movement, 128 Kbps in a car, and 2 Mbps in fixed applications.

The 3G technology specifications also promote the potential for a uniform, worldwide standard. 3G technologies will operate over or expand existing 2G wireless air interfaces such as Global System for Mobile Communications (GSM), the primary non-proprietary cellular technology used throughout the world today. GSM uses a variation of the time division multiple access (TDMA) protocol. Data is digitized, compressed, and then sent through a channel with two other streams of user data, each in its own time slot. Currently available circuit-switched GSM networks can transmit data at 9.6 Kbps. In the future it may be possible for GSM networks to transmit data at up to 43.2 Kbps using multiple time slot, high-speed circuit-switched data upgrades. Presently, GSM networks operate at either the 900 megahertz (MHz), 1.8 GHz or 1.9 GHz frequency band.

The advancement of GSM into 3G technologies is wideband code division multiple access (W-CDMA), which promises much higher data speeds. W-CDMA can support mobile voice, images, data, and video communications at up to 2 Mbps (local-area access) or 384 Kbps (wide-area access). The input signals are digitized and transmitted in a coded, spread-spectrum mode over a range of frequencies. A 5 MHz-wide carrier is used, rather than the 200 kHz-wide carrier used for narrowband CDMA.

Another 2G wireless air interface is CDMA (code division multiple access). CDMA, a form of multiplexing, allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth. The technology is used in cellular telephone systems in the 800 MHz and 1.9 GHz bands.

The evolution of current CDMA into 3G technologies in the short term is represented by 1xRTT (first-generation radio transmission technology). Eventually 1xRTT will further evolve to 3xRTT (third-generation radio transmission technology). These radio transmission technologies are enhancements of CDMA2000. 1xRTT will support mobile voice, images, data, and video communications at up to 144 Kbps. 3xRTT will transmit data at rates upwards of 384 Kbps for mobile and 2 Mbps for stationary applications. Currently, development of 3xRTT remains in the planning stages.

In Europe, the GSM network covering the Continent will likely be replaced with W-CDMA. Japan has also embraced W-CDMA technologies, where carrier NTT DoCoMo has an

estimated $8 billion invested in a nationwide W-CDMA network. A limited trial is under way with mixed results for the system's 4,000 users. China and South Korea appear ready to embrace CDMA2000 networks.

GSM-based packet radio services (GPRS), now being deployed in the United States, are already extremely popular throughout Europe. GPRS is a 2.5G evolution of GSM. With GPRS, the data is broken up into packets, rather than the continuous stream of data found in GSM circuit-switched networks, and offers "always on" connectivity. GPRS is of primary importance to the provision of mobile Internet capabilities that may deliver voice, video, and data to users at speeds up to 115 Kbps. In Europe, GPRS-equipped handsets are projected to be available for the mass market by early 2002. Availability in the United States may follow in mid-to-late 2002.

The next major 2.5G development for GSM is enhanced data rates for global evolution (EDGE), which purports to provide a 384 Kbps capability. EDGE is a new modulation scheme for the air interface that retains the basic frame structure of GSM and uses GPRS packet data protocols. EDGE technology is being developed specifically to meet the bandwidth needs of 3G applications. EDGE is more important to GSM providers that have not or could not acquire 3G technology licenses.

3G technology encompasses a wide variety of wireless standards, including (but not limited to) CDMA2000, GPRS, Universal Mobile Telecommunications Service (UMTS), TDMA, and W-CDMA, all of which are being considered for deployment in the United States.

Deployment of 3G technologies in the United States remains uncertain and somewhat fractured. The confusion lies in the multitude of wireless carriers and network infrastructure currently in use in North America, as well as the state of the spectrum ownership in the United States. Verizon Wireless and Sprint PCS are separately testing a variant version of CDMA2000 called 1XRIT. This technology will double the voice capacity of the current CDMA systems and increase the speed of the data networks to 144 Kbps. VoiceStream has selected W-CDMA because it has better compatibility with the present GSM network, while AT&T has indicated that they will use both W-CDMA and TDMA-EDGE. Cingular Wireless has not made a 3G-network decision public, while Nextel is continuing to contemplate how to convert its Motorola Integrated Dispatched Enhanced Network (iDEN) to high-speed 3G technologies.

Handset manufacturers are expediting development of entry-level 3G cellular devices that promise the delivery of voice, data, e-commerce, and wireless Internet and intranet access to users anytime, anywhere. They may eventually replace much of what is now performed on a desktop PC, laptop, or personal digital assistant (PDA).

One of the first 3G applications may be multimedia messaging service (MMS), which lets users record text messages synchronized with audio and video, and transmit them via cellular telephones or other handheld devices. Additionally, manufacturers and application developers are positioning to deliver real-time, interactive, multiple-player gaming over a wireless device that will support 2.5G and 3G technologies.

The deployment of infrastructures capable of supporting 3G technologies is of significant concern to existing carriers with deployed 2G or 2.5G systems. A high-capacity 3G network may be deployed as a parallel network, requiring different base stations and many new or additional infrastructure sites. In many cases, 3G base stations may be collocated with existing low-capacity GSM base stations, thereby leveraging existing sites, towers, and communications links.

Once these networks are in place, users will be required to upgrade to new devices to support desired bandwidth and applications. These devices may come with a high price tag—preliminary estimates for the first 3G devices range from $250 to $600, with monthly data plan rates ranging anywhere from $60 to $100.

ACRONYMS

1xRTT	First-Generation Radio Transmission Technology
3G	Third Generation
3xRTT	Third-Generation Radio Transmission Technology
AOL	Automatic Officer Location
APCO	Association of Public Safety Communications Officials–International, Inc.
AVL	Automatic Vehicle Location
bps	Bits per Second
CAD	Computer-Aided Dispatch
CapWIN	Capital Wireless Integrated Network
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
EDGE	Enhanced Data Rates For Global Evolution
EMS	Emergency Medical Services
ESMR	Enhanced Specialized Mobile Radio
ETSI	European Telecommunications Standards Institute
GHz	Gigahertz
GIS	Geographic Information System
GPRS	GSM-Based Packet Radio Services
GSM	Global System for Mobile Communications
iDEN	Integrated Dispatched Enhanced Network
Kbps	Kilobits per Second
LAN	Local Area Network
Mbps	Megabits per Second
MDC	Mobile Data Computer
MDD	Mobile Data Device
MDT	Mobile Data Terminal
MESA	Mobility for Emergency and Safety Applications
MHz	Megahertz
MMS	Multimedia Messaging Service
MST	Mobile Status Terminal
NASTD	National Association of State Telecommunications Directors
NCIC	National Crime Information Center
NLETS	National Law Enforcement Telecommunications Systems
P34	Project 34
PAN	Personal Area Network
PCS	Personal Communications Services
PDA	Personal Digital Assistant
PSWN	Public Safety Wireless Network
RFP	Request for Proposals
RMS	Records Management System
SDO	Standards Development Organization
SMR	Specialized Mobile Radio
TDMA	Time Division Multiple Access
TETRA	Terrestrial Trunked Radio
TIA	Telecommunications Industry Association
UMTS	Universal Mobile Telecommunications Service
W-CDMA	Wideband Code Division Multiple Access